MARCELO EDUARDO DA SILVA MOREIRA 96/18368
RÔMULO FACURI MIRANDA CORDEIRO 98/31185

DESENVOLVIMENTO DE PROCEDIMENTOS DE SEGURANÇA E IMPLANTAÇÃO DE FIREWALL NO LABORATÓRIO DE BIOINFORMÁTICA DA REDE GENOMA CENTRO-OESTE

Trabalho de graduação apresentado ao Curso de Ciências da Computação, Instituto de Ciências Exatas, Universidade de Brasília.
Orientador: Mestre João José Costa Gondim

BRASÍLIA

2002

Projeto final sob o título “Desenvolvimento de Procedimentos de Segurança e Implantação de Firewall no Laboratório de Bioinformática da Rede Genoma Centro-Oeste”, defendida por Marcelo Eduardo da Silva Moreira e Rômulo Facuri Miranda Cordeiro e aprovada em 11 de setembro de 2002, em Brasília, Distrito Federal, pela banca examinadora constituída pelos professores:

Prof. Mestre João José Costa Gondim

Orientador

Profª. Drª. Maria Emília Machado Telles Walter

Universidade de Brasília

Prof. Dr. Luiz Antônio da Frotta Matos

Universidade de Brasília

Prof. Dr. Marcelo de Macedo Brígido

Universidade de Brasília

Agradecimentos

A elaboração de um projeto de graduação requer muita dedicação e esforço, e este não foi diferente. Mais do que isso, este projeto foi um desafio para nós. Muitas foram as vezes que deixamos de lado outros compromissos para poder dar continuidade a nosso trabalho.

Gostaríamos inicialmente de agradecer ao professor e orientador Gondim, que esteve conosco colaborando, disponibilizando seu tempo e dando seu apoio fundamental. Como jovens “Padawans”, estivemos sempre tentando assimilar aquele conhecimento adicional que nosso mestre poderia nos trazer. Gostaríamos também de agradecer à professora Maria Emília, pelas sugestões e suporte dado.

Neste caminho que percorremos, muitos foram aqueles que vieram em nosso auxílio, alguns trazendo apoio técnico, outros trazendo apoio psicológico. Em especial, gostaríamos de agradecer às seguintes pessoas: Leila Aparecida, Sonia Maria e Manoel Netto, nossos pais; Daniele Beust, por entender os sacrifícios e ausências durante o semestre; Alex Rodrigues, como um grande incentivador e amigo; aos nossos irmãos, parentes e amigos de computação, nosso muito obrigado.

Finalmente, gostaríamos de agradecer a Deus, por nossa existência e também a de todas as pessoas que estão conosco. A seguir, destacamos um pensamento de outro grande mestre:

“Um estudante Jedi deve ser humilde em seu poder, amadurecer o suficiente para abraçar a responsabilidade que vem com o domínio da Força. Um estudante talentoso, impaciente com exercícios insensatos, ansioso com a lentidão de seu tutor, pode perder o ponto para se tornar um Jedi. O Jedi não almeja poder, mas busca servir outros, sem a expectativa de formação de ser poderoso na Força”

Mestre Luke Skywalker

Sumário

Capítulo 1 – Introdução

1.1. Introdução à segurança dos sistemas de informação

O crescimento dos computadores e da tecnologia da informação tem sido explosivos. Nunca antes uma tecnologia inteiramente nova se propagou por todo o mundo em uma velocidade tão grande e com tanta penetração em praticamente toda atividade humana. Computadores trouxeram vastos benefícios a inúmeras áreas como o estudo do genoma humano, exploração espacial, inteligência artificial, bem como todo um conjunto de aplicações, das mais triviais até as mais importantes à vida.

Infelizmente, existe um lado ruim do uso dos computadores: Eles podem ser empregados para desenvolver armas de destruição em massa, submarinos nucleares e também aeronaves militares.

Computadores são também utilizados em aplicações financeiras, facilitando a compra e venda de qualquer coisa, desde palitos de fósforo até mansões, e transferindo trilhões de dólares todos os dias em fundos. Porém, muitos vêem estas atividades como convites à fraude e ao roubo. Sistemas computacionais e suas redes de interconecção são também vítimas de: vândalos, ataques maliciosos, terroristas, bem como pessoas, grupos ou governos intencionados a usar os sistemas computacionais para seus próprios fins. Além destes problemas de ataques intencionais, existem inúmeros modos pelos quais erros inadvertidos podem prejudicar ou destruir a capacidade computacional em desempenhar atividades desejadas.

Em função destes problemas de segurança, o crescimento necessidade de segurança dos sistemas de informação têm sido paralelo ao próprio crescimento dos computadores. Apenas com um estudo detalhado dos problemas potenciais e implementação das alterações sugeridas, os computadores poderão ter a capacidade de atender às expectativas voltadas a eles.

Segurança pode ser definida como o estado de estar livre de perigo e não exposto ao perigo de acidentes ou ataques, ou isto pode ser definido como o processo de aquisição deste estado desejável [9]. O objetivo da segurança dos sistemas de

informação é otimizar a performance de uma rede, seja esta de um laboratório ou organização, respeitando os riscos aos quais ela está exposta.

Risco é definido como a chance de prejuízo, perigo ou perda. Assim, risco possui dois elementos [9]:

- Elemento de incerteza;
- Perda ou prejuízo.

A não ser pela possibilidade de restituição, as ações dos Sistemas de Segurança da Informação (SSI) tomadas hoje trabalham para reduzir riscos de perda futuros. Em função da incerteza dos riscos no futuro, a segurança perfeita, que implica perda zero, seria infinitamente cara. Por esta razão, gerenciadores de risco em SSI se esforçam por otimizar a alocação de recursos, minimizando o custo total das medidas de SSI tomadas e o risco das perdas experimentadas.

Neste contexto de Segurança da Informação, um elemento que possui importância chave no Projeto de Segurança de qualquer rede que necessite de proteção contra ações externas indesejáveis é o Firewall. Um Firewall dá a uma rede uma forma de se criar um meio termo entre redes que são isoladas e redes externas, tais como a Internet, e estas que são completamente conectadas. Colocado entre a rede interna e a rede externa, o Firewall fornece uma maneira simples de controlar a quantidade e as formas de tráfego que irão passar entre as duas redes.

O termo Firewall é também aplicado à indústria de construção. Quando um apartamento ou escritório é construído, ele pode ser equipado com um Firewall (parede de fogo), sendo estas paredes especialmente construídas e resistentes ao fogo.

A mesma filosofia pode ser aplicada à proteção de uma rede local contra ataques a máquinas localizadas na rede externa. Usado dentro de uma organização, um Firewall pode reduzir o volume de prejuízo: um intruso pode invadir um conjunto de máquinas, mas o Firewall irá proteger outro conjunto. Levantado entre a rede interna e a externa, um Firewall pode prevenir um invasor malicioso, que já obteve acesso a computadores da rede externa, de obter um ponto de apoio internamente.

O presente projeto teve como objetivos o Desenvolvimento de Procedimentos de Segurança e a implantação de um Firewall no Laboratório de Bioinformática (BIOINFO) da Rede GENOMA Centro-Oeste.

Na criação dos Procedimentos de Segurança, utilizou-se como base os modelos de políticas existentes: *RFC2196* [3] (*Site Security Handbook*) e o *IT Baseline Protection Manual* [4]. Além destes, foi também utilizado como referência um questionário existente no capítulo 46 do "*Computer Security Handbook*" [10].

Para a implantação do Firewall, utilizou-se o OpenBSD (sistema operacional) versão 3.11, o qual foi instalado em uma máquina dedicada, contendo 3 interfaces de rede e o *Packet Filter* para realizar a filtragem dos pacotes. Este foi primeiramente instalado em uma máquina de teste no laboratório. Posteriormente à esta instalação e verificação de seu funcionamento adequado, foi feita a instalação do sistema operacional na máquina definitiva e migração da configuração da máquina de testes para esta.

Este trabalho foi estruturado de forma que, nos capítulos iniciais (Capítulos 2 e 3), fosse levantado um arcabouço teórico para as duas partes práticas do projeto. No Capítulo 2 são explanadas as linhas de base sobre o planejamento de necessidades de segurança, avaliação dos riscos bem como os modelos de proteção e os princípios de segurança de uma rede conectada à Internet. O Capítulo 3 aborda os conceitos de Firewall, suas indicações, contra-indicações e utilização do *Packet Filter*.

Uma vez de posse dos conceitos de segurança abordados no Capítulo 2, o Capítulo 4 inicia a parte prática do projeto, a qual se refere ao Desenvolvimento dos Procedimentos de Segurança. Este Capítulo é dividido em 3 partes: Avaliação Preliminar (FASE 1 - Levantamento de Dados); Descrição da Situação Atual (FASE 2) e os Procedimentos de Segurança (FASE 3).

Finalizando a parte prática do projeto, o Capítulo 5 aborda a Implantação do Firewall, descrevendo as etapas de instalação, configuração da rede e implantação das regras de filtragem.

O Capítulo 6 é destinado a uma descrição das dificuldades encontradas nas etapas de Desenvolvimento dos Procedimentos de Segurança e Implantação do Firewall, bem como sugestões para trabalhos futuros.

A Conclusão do Trabalho é feita no Capítulo 7, onde se tem um fechamento sobre os resultados obtidos na Implementação do Firewall e na apreciação das Medidas de Segurança propostas. Após este capítulo segue o Anexo 1 (contendo o Questionário de Avaliação Preliminar), o Anexo 2 (contendo a lista de tabelas), o Anexo 3 (contendo a lista de ilustrações) e as Referências Bibliográficas. Nesta última encontram-se todas as fontes consultadas para estudo, elaboração e implantação da parte prática, bem como deste documento.

Capítulo 2 – Segurança de redes e Internet

Fundamentalmente, segurança computacional consiste em uma série de soluções técnicas para problemas não técnicos. Pode-se gastar uma ilimitada quantidade de tempo, dinheiro e esforço em segurança computacional, mas nunca será resolvido o problema de perda de dados acidentais ou uma interrupção intencional de suas atividades. Dadas as devidas circunstâncias – "*bugs*" de software, acidentes, erros, má sorte, mau tempo ou um invasor bem motivado e bem equipado – qualquer computador pode ficar comprometido, submetido a desuso ou algo pior do que isso.

A função dos profissionais de segurança é auxiliar organizações a decidir quanto tempo e dinheiro precisam ser gastos com segurança. A outra parte do trabalho é assegurar que as organizações possuam políticas, orientações básicas e procedimentos para que o dinheiro seja bem gasto. E finalmente, o profissional precisa auditar o sistema para assegurar que os controles apropriados estão implementados corretamente para alcançar os objetivos da política. Deste modo, a segurança prática é realmente uma questão de gerenciamento e administração mais do que uma habilidade técnica. Consequentemente, a segurança deve ser prioridade no gerenciamento de uma rede de computadores.

Existem dois princípios críticos implícitos na política efetiva e planejamento de segurança [9].

- Política e qualidade de segurança devem ser dirigidas de "cima para baixo" no local a ser implantado. Preocupações com segurança e qualidade pelos usuários são importantes, mas elas não podem construir ou sustentar uma cultura efetiva de segurança. Ao invés disso os chefes de organizações devem tratar a segurança como algo de suma importância e acatá-la em todas as regras e regulamentações como todos os outros.
- Segurança computacional efetiva significa proteger *informação*. Todos os planos, políticas e procedimentos devem refletir a necessidade de proteger informação de qualquer forma. Os dados não se tornam sem importância quando impressos ou enviados via fax para outro local ao invés de estarem

contidos em um arquivo no disco. A informação confidencial interpessoal não perde seu valor, repentinamente, se for falada no telefone entre dois usuários ao invés de estar contida num correio eletrônico. A informação deve ser protegida não importando a sua forma.

2.1. Planejando As Necessidades De Segurança

Existem vários diferentes tipos de segurança computacional, e várias diferentes definições. Mais do que apresentar apenas uma definição formal, este trabalho aborda uma aproximação prática e discute as categorias de proteção que devem ser consideradas. Computadores seguros são também computadores de uso e, do mesmo modo, computadores que não podem ser usados, por qualquer razão, não são muito seguros.

Dentro desta abordagem, existem vários e diferentes tipos de segurança que tanto usuários, quanto administradores de sistemas de computadores devem se preocupar [9].

Confidencialidade

- Proteger informação de ser lida ou copiada por qualquer um que não está explicitamente autorizado pelo dono da informação. Este tipo de segurança inclui não somente proteger a informação como um todo e sim proteger pedaços individuais de informação que podem ser inofensivos por eles mesmos mas que podem ser usadas para inferir outra informação confidencial.

Integridade dos Dados

- Corresponde a proteger a informação (inclusive programas) de serem apagados ou alterados de alguma forma sem a permissão do proprietário da informação. Proteção da informação também inclui proteger itens como

registro de contas, fitas de “backup”, número de vezes que o arquivo foi criado e documentação.

Disponibilidade

- Proteger os serviços para que eles não fiquem degradados ou indisponíveis sem autorização. Se o sistema está indisponível quando um usuário autorizado precisa dele, o resultado pode ser pior do que se uma informação que reside no sistema fosse apagada.

Consistência

- Assegurar-se que o sistema comporta-se como esperado pelos usuários autorizados. Se o software ou o hardware repentinamente começa a se comportar de uma maneira radicalmente diferente daquela que se costuma comportar, especialmente após uma atualização ou a reparação de um erro, pode ocorrer um desastre. Seria um grande problema se o comando “ls” ocasionalmente apagasse arquivos ao invés de listá-los. Este tipo de segurança também pode ser considerado como assegurar a exatidão dos dados e do software que está sendo utilizado.

Controle

- Regular acesso ao sistema. Se indivíduos (ou software) desconhecidos ou não autorizados são encontrados no sistema, eles podem criar um grande problema. Deve-se preocupar como entraram, o que devem ter feito e quem ou o que mais também acessou o sistema. Recuperar-se destes episódios pode requerer consideráveis tempo e gasto para reconstruir e reinstalar o sistema e ainda verificar se nada de importante foi mudado ou revelado – mesmo se nada aconteceu de fato.

Auditoria

- Tal como preocupar-se com usuários não autorizados, os usuários autorizados às vezes cometem erros, ou até mesmo atos maliciosos. Nesses casos deve-se determinar o que foi feito, por quem, e o que foi afetado. A única maneira de se alcançar estes resultados é através de alguns registros incorrompíveis de atividade no sistema que indiscutivelmente identifica os autores e ações envolvidas. Em algumas aplicações críticas, a trilha da auditoria pode se estender à autorização de operações que desfaçam ou ajudem a restaurar o sistema ao seu estado correto.

Embora todos estes aspectos de segurança sejam importantes, organizações diferentes visualizarão, cada qual com um diferente nível de importância. A variação é devida porque diferentes organizações têm diferentes preocupações e devem direcionar suas prioridades e políticas de acordo com suas necessidades. Por exemplo:

- Num ambiente bancário, integridade e auditoria são geralmente as preocupações mais críticas, enquanto a confidencialidade e disponibilidade são as seguintes no nível de importância.
- Num sistema nacional relacionado à defesa o qual processa informação classificada, confidencialidade vem primeiro e disponibilidade vem por último.
- Numa universidade, integridade e disponibilidade podem ser os requisitos mais importantes. A prioridade é dada aos estudantes para trabalharem em seus projetos ao invés de monitorar o horário exato que os estudantes acessaram suas contas.

Para um administrador de segurança, é necessário entender completamente as necessidades de seu ambiente operacional e de seus usuários. Este então precisará definir os procedimentos conformemente. Nem tudo que descrevemos nesse trabalho terá aplicação direta a qualquer ambiente.

Confiança

Profissionais de segurança, geralmente não se referem a um sistema de computador como sendo "seguro" ou "inseguro". Ao invés disso, é usada a palavra "confiável" para descrever o nível de confiança no qual o sistema computacional se comporta. Isto reconhece que a segurança absoluta nunca estará presente. Desenvolver confiança adequada em um sistema computacional requer um pensamento cuidadoso e planejado. As decisões devem ser baseadas nas decisões políticas e análise de risco.

Avaliação de Risco

O primeiro passo para melhorar a segurança de um sistema é responder as questões básicas que seguem abaixo.

- O que estou tentando proteger?
- De quem eu devo proteger?
- Quanto tempo, esforço e dinheiro eu estou pretendendo gastar para obter a proteção adequada.

Essas questões formam a base do processo conhecido como avaliação de risco. A avaliação de risco é uma parte muito importante da segurança computacional. Não se pode proteger a si mesmo se não é do conhecimento contra o que se protege. Após saber dos riscos existentes, pode-se planejar as políticas e técnicas que serão necessárias para implementar e reduzir estes riscos.

Por exemplo, se existe o risco de falha de energia e se a disponibilidade do equipamento é importante, pode-se reduzir os riscos adquirindo um dispositivo UPS (*Uninterruptable Power Suply*).

O risco não pode ser eliminado

É possível identificar e reduzir os riscos, mas nunca poderá eliminá-los por inteiro. Por exemplo, pode-se comprar um dispositivo de força ininterrupta para reduzir o risco de falha de energia, deteriorando seus dados. Mas este dispositivo pode falhar quando você precisar dele; a interrupção de energia pode ser maior do que a capacidade de sua bateria; o pessoal de limpeza pode desplugar o cabo de força no momento de lavar o chão, etc.

Uma avaliação do risco cuidadosa identificará estes riscos secundários e irá ajudá-lo a fazer planos para eles. Pode-se comprar um segundo dispositivo de ininterruptabilidade de força, mas existe ainda a possibilidade dos dois falharem ao mesmo tempo.

Avaliação dos riscos pode ajudar a se proteger e proteger uma rede contra riscos humanos e naturais. Pode-se usar a avaliação de risco para efetivar a proteção contra quebra de computadores, identificando os riscos e planejando de acordo, mas falhas de energia não se pode eliminar completamente.

Este fato é fundamental para a segurança computacional. Não importa quão seguro esteja um computador, este poderá ser invadido se forem usados recursos suficientes, tempo, motivação e dinheiro.

Quatro passos simples para uma melhor segurança de computadores

Fazer um computador seguro é um trabalho árduo. De maneira geral, recomenda-se ao menos seguir estes quatros passos simples:

1. Decida quão importante a segurança é para o local. Caso a segurança seja muito importante e o local sofrerá perdas significativas no caso de uma ruptura na segurança, deve ser dada uma certa prioridade a esta resolução. Associar um programador sobrecarregado de trabalho o qual não tem a menor intimidade para tomar conta da segurança, é sem dúvida, uma incitação à problemas.

2. Envolver e educar a comunidade de usuários. Os usuários no local de trabalho compreendem os perigos e riscos envolvidos com práticas de segurança? Os usuários devem saber o que e quem chamar se observarem alguma coisa suspeita ou desapropriada. Educar a população de usuários ajuda-os a fazer deles parte da segurança. Manter os usuários mal informados das limitações do sistema e das operações não aumentará a segurança do sistema - existem sempre outras fontes de informações para determinados invasores.
3. Planejar uma maneira de fazer e armazenar backups dos dados do sistema. Deve-se ter backups periódicos, com informação sobre as datas dos mesmos, bem como fazer uma rotina de verificação dos dados contidos nas mídias.
4. Estar alerta e suspeitar de tudo. Se alguma coisa aparentemente incomum acontecer, deve-se suspeitar de um intruso e investigar. Geralmente o problema trata-se de uma falha ou erro no sistema. Mas ocasionalmente pode-se descobrir algo mais sério. Por esta razão, cada vez que alguma coisa acontece e definitivamente não se consegue explicar, deve-se suspeitar de um problema de segurança e investigá-lo.

Administrar o risco é usar o bom senso

É crucial, para uma boa avaliação de risco, identificar todas as possíveis ameaças ao sistema, mas apenas se defender contra aqueles ataques que, na realidade, sejam ameaças verdadeiras.

Só porque pessoas são o ponto fraco quando se fala em segurança de sistemas, isso não significa que devemos ignorar outras medidas de segurança. Pessoas são imprevisíveis, mas conseguir invadir um modem discado que não é protegido por uma senha, sai mais barato que um suborno. Portanto, utilizam-se defesas tecnológicas onde for possível, e seja possível melhorar a segurança a nível de pessoal através da educação de funcionários e usuários.

Deve-se apostar na defesa em profundidade: aplicar níveis múltiplos de defesas como *backups*, caso algum falhe. Por exemplo, pode-se comprar um segundo sistema UPS ou colocar uma tranca separada na sala de computadores, mesmo que já exista

uma tranca na porta do prédio onde a sala se encontra. Embora esse tipo de combinação possa ser derrotada, isso implica num aumento de esforço e custo para o invasor, e isso talvez possa convencê-los que não vale a pena. No mínimo, tais medidas poderão retardá-los o suficiente para que os sistemas de monitoramento ou alarmes possam pedir ajuda antes que algum estrago maior seja feito.

Tendo em mente estes limites, deve-se encarar que a segurança de sistemas é um conjunto bem desenvolvido de prioridades. Não é possível se proteger contra todo tipo de ameaça. Às vezes é melhor deixar que o problema ocorra e limpar a bagunça depois, em vez de efetuar algum tipo de prevenção. Por exemplo, o esforço poderá ser menor e menos custoso deixando que o sistema caia durante uma falta de energia e depois reiniciar, do que comprar um sistema UPS. Vale lembrar que existem algumas coisas contra as quais nem vale a pena se defender, ou porque são muito improváveis que aconteçam (ex. uma invasão alienígena), muito difíceis de defender (ex. uma explosão nuclear a 800 metros do centro de dados), ou simplesmente catastróficas ou horríveis demais para contemplar (ex. a gerência decide trocar todas as maquinas UNIX para um sistema operacional bem conhecido).

A chave para um bom gerenciamento é conhecer as coisas que possam trazer alguma preocupação e qual o grau desta preocupação.

Deve-se decidir o que deve ser protegido e quais podem ser os custos para prevenir estas perdas *versus* o custo de recuperar-se destas perdas. Então, tomar as decisões para ações e medidas de segurança baseadas num lista priorizada pelas necessidades mais críticas.

2.6. Segurança de uma rede conectada à Internet

2.6.1. Modelos de proteção

2.6.1.1. Sem Segurança

A abordagem mais simples possível é não investir nenhum esforço em segurança, mantendo o nível de segurança padrão que já vem com a máquina.

2.6.1.2. Segurança por obscuridade

Outro modelo possível de segurança é aquele geralmente conhecido como "segurança por obscuridade". Com este modelo, um sistema estaria seguro em função (supostamente) de ninguém saber sobre ele - sua existência, conteúdos, medidas segurança ou qualquer outra coisa. Esta abordagem raramente dura muito tempo.

Muitas pessoas assumem que embora os invasores possam achá-los, eles não os aborrecerão. Eles imaginam que uma companhia pequena ou um computador doméstico não serão do interesse de intrusos. Na realidade, muitos intrusos não são levados por interesses particulares, eles simplesmente querem invadir tantas máquinas quanto possível. Para eles, companhias pequenas e computadores domésticos são vistos simplesmente como alvos fáceis.

Intrusos têm muito tempo em suas mãos e podem evitar quase sempre ter que descobrir fatos mais complexos simplesmente tentando todas as possibilidades. No final das contas, confiar em obscuridade não é uma escolha de segurança inteligente.

2.6.1.3. Segurança de Host

Provavelmente o modelo mais comum para segurança de computadores é segurança de host. Com este modelo, é aplicada a segurança em cada máquina de host separadamente, e todo esforço é feito para evitar ou aliviar os problemas de segurança conhecidos que poderiam afetar aquele host em particular. O problema com

a segurança de host não é a efetividade desta, mas que ela fica pouco viável em grandes instalações com um número elevado de host.

O impedimento principal à segurança de host em ambientes de computação modernos é a complexidade e diversidade desses ambientes. A maioria dos ambientes modernos inclui máquinas de diversos vendedores, cada um com seu próprio sistema operacional, e seu próprio conjunto de problemas de segurança. Até mesmo se o local possuir máquinas de só um vendedor, versões diferentes do mesmo sistema operacional têm problemas de segurança significativamente diferentes. Até mesmo se todas estas máquinas são de um único vendedor e tem a mesma versão do sistema operacional, configurações diferentes (serviços diferentes habilitados, e assim por diante) podem trazer conjuntos de subsistemas diferentes, o que conduz a conjuntos diferentes de problemas de segurança. E, até mesmo se as máquinas forem absolutamente idênticas, a grande quantidade deles em alguns locais pode fazer a segurança ser muito complexa.

Segurança de host também diz respeito às boas intenções e ao nível de acesso que cada um tem para uso da máquina. Na medida em que o número de máquinas aumenta, o número de usuários privilegiados geralmente aumenta também. Fazer a segurança de uma máquina é muito mais difícil do que atacá-la em uma rede.

Um modelo de segurança de host pode ser apropriado a locais pequenos, ou locais com exigências de segurança extremas.

2.6.1.4. Segurança de Rede

Na medida em que os ambientes crescem e se diversificam, e na medida em que a segurança host a host se torna mais complexa, cresce o uso do modelo de segurança de rede. Com um modelo de segurança de rede, o controle do acesso de rede é concentrado em seus vários hosts e os serviços que eles oferecem, em lugar de fazê-los um por um. A abordagem de segurança de rede inclui Firewalls para proteger os sistemas internos e redes, usando um sistema de autenticação forte e encriptação para

proteger dados particularmente sensíveis que transitam na rede. Assim, um local pode obter um tremendo reforço de segurança usando um modelo de segurança de rede.

2.6.1.5. Nenhum modelo de segurança pode fazer tudo

Nenhum modelo de segurança pode resolver todos os problemas. Para burlar um host seguro ou um bom modelo de segurança de rede, um indivíduo pode simplesmente usar métodos físicos. Estes podem ser até derramar refrigerante em seus teclados, com o intuito de impossibilitar a continuidade de seus afazeres no local de trabalho e poder levar documentos de alta confidencialidade para casa.

Nenhum modelo de segurança pode cuidar dos problemas de gerenciamento. A segurança dos computadores não impedirá as pessoas de desperdiçarem tempo ou chatearem uns aos outros.

Nenhum modelo de segurança provê proteção perfeita. Pode-se fazer com que as invasões sejam raras, breves, e com baixo ônus, mas não se pode esperar evitá-las completamente. Até mesmo os locais mais seguros e dedicados esperam ter um incidente de segurança em determinado momento.

A segurança pode não prevenir todos os incidentes, mas pode impedir que um incidente danifique seriamente ou deixe fora de operação determinado sistema.

2.6.2. Princípios aplicáveis à segurança de redes conectadas à Internet

2.6.2.1. Menos privilégio

Talvez, o princípio mais fundamental de segurança é o de menos privilégio. Basicamente, o princípio de menos privilégio diz que um objeto (usuário, administrados, programa ou mesmo sistema) deveria ter apenas os privilégios necessários para que este possa realizar suas tarefas. Menos privilégio é um princípio importante na limitação da exposição de sistemas contra ataques, e para limitar o estrago causado por formas particulares de ataques.

No contexto de Internet, existem vários exemplos de restrição de privilégio. Provavelmente:

- Todo usuário não precisa acessar todos os serviços de Internet existentes;
- Todo usuário não precisa modificar todos os arquivos em seu sistema;
- Todo usuário não precisa saber a senha de root (administrador) da máquina.
- Todo administrador de sistema não precisa conhecer as senhas de root de todos os sistemas;
- Todo sistema não precisa acessar todos os arquivos de todo outro sistema.

A aplicação do princípio de menos privilégio sugere que se deva explorar modos para reduzir os privilégios requeridos para várias operações. Por exemplo:

- Não dar para um usuário a senha de root para um sistema se tudo que este usuário precisa fazer é reiniciar a impressora;
- Não confiar ao Firewall a tarefa de fazer backups em outras máquinas. Ao invés disso, colocar um dispositivo de backup no próprio Firewall para que este possa executar seus próprios backups.

Muitas das soluções empregadas na proteção dos sistemas são táticas da estratégia de menos privilégio. Por exemplo, um sistema de filtragem de pacotes (Packet Filtering) é projetado para permitir os pacotes dos serviços que se deseja garantir acesso.

Existem dois problemas na tentativa de gerar menos privilégio. Primeiro, pode ser complexo implementar quando esta não é uma característica já existente dos programas e protocolos em uso (no caso do Windows). A tentativa de implementar este recurso pode ser muito complicada. Outro problema é ocasionado em função da possibilidade de se implementar algo que gera um nível de privilégio menor do que o necessário.

2.6.2.2. Ponto de Convergência

Um ponto de convergência (choke point) força os invasores a usar um canal estreito que se pode monitorar e controlar. Em segurança de rede, o Firewall entre determinado sistema e a Internet (assumindo que é a única conexão entre este local e a Internet) é um ponto de convergência. Qualquer um que tente atacar este local a partir da Internet vai ter que passar por aquele canal supostamente protegido. Porém, um ponto de convergência é inútil se houver um modo efetivo para um invasor sobrepujá-lo.

2.6.2.3. Link mais fraco

Uma doutrina fundamental de segurança é que uma cadeia é tão forte quanto sua ligação mais fraca e uma parede é tão forte quanto seu ponto mais fraco. Invasores inteligentes vão procurar aquele ponto fraco e concentrar suas atenções nele. Deve-se estar atento aos pontos fracos da defesa do sistema de forma que se possa tomar as medidas para eliminá-los, e de forma que se possa monitorar os pontos vulneráveis que não se pode eliminar.

Sempre haverá um link mais fraco, porém, a idéia é fazer aquela ligação forte o bastante e manter a força proporcional ao risco. Por exemplo, é razoável ter mais preocupação com tentativas de invasão externas pela rede do que com problemas de ataque físico à esta. Desta forma, pode-se permitir que a segurança física seja a ligação mais fraca. Porém, não é razoável negligenciar a segurança física completamente.

Modelos de segurança de host sofrem de uma peculiaridade no que diz respeito à relação entre ligação mais fraca e ponto de convergência. Neste modelo não há nenhum ponto de convergência, o que significa que existem vários links a este host, e algum deles podem ser realmente fraco.

2.6.2.4. Participação de todos

Para ser completamente efetivo, a maioria sistemas de segurança requerem a participação universal (ou pelo menos a ausência de oposição ativa) do pessoal local. Se alguém optar por não utilizar os mecanismos de segurança implantados, então um

invasor pode primeiramente atacar o sistema daquela pessoa isenta de segurança e após invadi-lo, direcionar o seu foco para o restante da rede.

Deve-se solicitar a todos que reportem problemas de segurança que porventura estejam ocorrendo, não se pode ver tudo. É necessário que as pessoas escolham senhas fortes, mudem-nas com regularidade e não as distribuam para seus amigos ou mesmo parentes.

A participação de todos deve ser voluntária ou involuntária, ou até uma combinação das duas. Obviamente, participação voluntária é preferível à involuntária.

2.6.2.5. Simplicidade

Simplicidade é uma estratégia de segurança por duas razões. Primeiramente, manter as coisas mais simples as torna mais fáceis de se entender. Se algo não é compreendido, não se pode realmente saber se o mesmo é ou não seguro. Segundo, complexidade provê todo tipo de condições para que coisas fora de conhecimento estejam ocultadas. É mais fácil fazer a segurança de um quarto e sala do que de uma mansão.

Programas complexos tem mais bugs, sendo que cada um deles pode constituir um problema de segurança. Mesmo que os bugs não constituam um problema de segurança, uma vez que as pessoas esperem um funcionamento anormal do computador, elas irão aceitar qualquer comportamento deste, o que anula qualquer possibilidade de se reconhecer e reportar problemas de segurança quando estes surgirem.

2.7. Conclusão

Neste capítulo, são relatadas as mais diversas formas de segurança de redes. É feita uma abordagem sobre suas necessidades, avaliação dos seus riscos e são evidenciados os modelos de proteção que podem ser implementados. Além disso, são abordados modelos de proteção e os princípios de segurança de uma rede conectada à Internet.

Capítulo 3 - Firewalls

Em construções, uma parede de fogo tem como função impossibilitar o fogo de passar de uma parte da construção para outra. Em teoria, um Firewall de Internet serve a um propósito similar: Ele previne possíveis perigos originados da Internet de passarem para a rede interna. Na prática, um Firewall de Internet é mais como um fosso de um castelo medieval em um prédio moderno. Ele serve a múltiplos propósitos:

- Restringe a entrada de dados utilizando um ponto de acesso controlado.
- Evita que os invasores cheguem perto dos sistemas em questão.
- Restringe a saída de dados utilizando um ponto de acesso controlado.

Um Firewall de Internet é mais freqüentemente instalado no ponto de proteção da rede interna à Internet, conforme figura 3.1
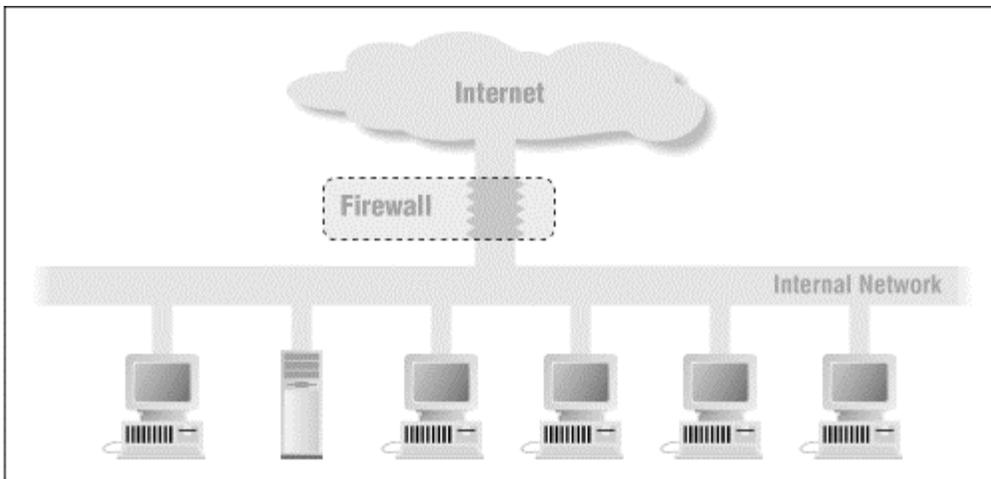
Figura 3.1: Um Firewall geralmente separa a rede interna da Internet

Todo o tráfego originário da Internet, ou indo para esta, passa através do Firewall. Desta forma, o Firewall tem a oportunidade de garantir que este tráfego seja aceitável.

Para o Firewall, “aceitável” quer dizer que, aquilo que esteja sendo feito: e-mail, transferência de arquivos, login remoto ou qualquer outro tipo de interações específicas

entre sistemas está em conformidade com a política de segurança do Firewall. Políticas de segurança são diferentes para cada localidade, algumas são altamente restritivas, porém, outras são altamente abertas.

De maneira lógica, o Firewall é um separador, um mecanismo de restrição, um analisador. A implementação física do Firewall varia de local para local. Mais freqüentemente, um Firewall é um conjunto de componentes de hardware: um roteador, um host ou uma combinação de roteadores, computadores e redes com o software apropriado. Existem várias formas de configurá-lo; a configuração dependerá da política local de segurança e dos serviços utilizados.

Tal como um fosso de um castelo medieval, o Firewall não é invulnerável. Este pode ter vulnerabilidade e limitações na proteção que oferece. O Firewall trabalha melhor se em conjunto com outras defesas internas. Um Firewall também tem suas desvantagens, durante sua implementação, os momentos de ajustes de permissão de acesso causam momentos onde a comunicação com a rede externa pode ficar inoperante, fato este que causa aborrecimentos aos usuários.

Mesmo com as limitações e desvantagens dos Firewalls, sua implementação se faz necessária, pois este é o modo mais efetivo para conectar uma rede à Internet e ainda proteger aquela rede. A Internet apresenta oportunidades maravilhosas. Milhões de pessoas trocam informação nesta. Os benefícios são óbvios: existem chances para publicidade, atendimento ao consumidor e troca de informações. A popularidade da estrada da informação mundial está aumentando, assim como o desejo de acesso seguro. Os riscos também são óbvios: A existir a possibilidade de se comunicar com milhões de pessoas, também existe a possibilidade de ser vítima. Qualquer rodovia expressa só é divertida enquanto se está dentro do carro. Ter que andar ou trabalhar na rodovia, pode ser perigoso.

3.1. Possibilidades de uso de Firewalls

Firewalls podem fazer muito para a segurança de uma rede conectada à Internet. De fato, algumas vantagens do uso de Firewalls vão além da segurança.

3.1.1. O Firewall é o foco para decisões de segurança

O Firewall é como um ponto de convergência. Todo o tráfego interno e externo tem que atravessar este posto de fiscalização. Um Firewall dá um grande salto na segurança de rede porque concentra as medidas de segurança neste posto de fiscalização: o ponto onde a rede se conecta à Internet.

3.1.2. O Firewall pode reforçar a política de segurança

Muitos dos serviços que as pessoas querem da Internet são inerentemente inseguros. O Firewall é quem policia o tráfego destes serviços. Ele reforça a política de segurança do local, permitindo que apenas os serviços "com aprovação" possam passar de fora para dentro e vice-versa.

Um Firewall pode ser utilizado para auxiliar políticas mais complicadas. Por exemplo, apenas alguns sistemas dentro do Firewall podem transferir arquivos para e da Internet. Assim, usando outros mecanismos para controlar quais usuários têm acesso a esses sistemas, pode-se controlar quais usuários têm estas capacidades.

Dependendo das tecnologias usadas na implementação do Firewall, este pode reforçar mais ou menos as políticas de segurança vigentes.

3.1.3. O Firewall pode fazer o log eficiente das atividades da Internet

Em função de todo tráfego passar pelo Firewall, este corresponde a um bom ponto de coleta de informações de tráfego para dentro e fora da rede protegida. Sendo um ponto de acesso único, o Firewall pode registrar aquilo que ocorre entre a rede interna e a rede externa.

3.1.4. O Firewall limita a exposição

Às vezes, um Firewall será usado para manter uma seção da rede local separada de outra seção. Fazendo isto, problemas que ocorrem em uma seção ficam restritos à esta, diminuindo a possibilidade de contaminação de outras seções. Em alguns casos, isto é feito porque uma seção exige mais segurança que outra, em outros casos, porque uma seção precisa ser mais acessada que outra. Qualquer que seja a razão, a existência do Firewall limita o dano que um problema de segurança de rede pode causar a toda a rede.

3.2. Limitações de uso de Firewalls

Firewalls oferecem grande proteção contra ameaças de rede, mas eles não são uma solução de segurança completa. Certas ameaças estão fora do controle dos Firewalls. Deve-se conhecer outras formas de proteção contra estas ameaças, tais como: incorporação de segurança física, segurança de host e educação de usuário no plano de segurança global.

3.2.1. O Firewall não pode proteger contra usuários internos mal-intencionados

Um Firewall deve impossibilitar um usuário de sistema de enviar informação restrita de uma organização pela conexão de rede, o que é feito pelas regras de restrição de tráfego. Mas aquele mesmo usuário poderia copiar os dados em disco, fita, ou papel e poderia levar isto para fora do edifício dentro de sua pasta.

Se o invasor já está dentro da rede interna, não há muito o que o Firewall possa fazer. Usuários internos podem roubar dados, causar dano em hardware e software, e sutilmente modificar programas sem ter que chegar sequer perto do Firewall. Ameaças internas requerem segurança interna de rede, como segurança de host e educação de usuário.

3.2.2. O Firewall não pode proteger contra conexões que não passam por ele

Um Firewall pode controlar o tráfego que passa por ele, porém, não há nada que um Firewall possa fazer sobre tráfego que não passa por ele. Por exemplo, caso seja permitido um acesso discado em sistemas internos à rede externa, o Firewall não tem como impedir uma invasão através desta conexão discada.

3.2.3. O Firewall não pode proteger contra ameaças novas

Um Firewall é projetado para garantir segurança contra ameaças conhecidas. Um modelo bem projetado também pode proteger contra algumas ameaças novas. Porém, nenhum Firewall pode defender automaticamente contra toda ameaça nova que surge. Periodicamente as pessoas descobrem modos novos para atacar, usando serviços previamente confiáveis, ou usando ataques que simplesmente não haviam ocorrido a ninguém. Não se pode montar um Firewall uma vez, e esperar que ele proteja para sempre.

3.2.4. Um Firewall não pode proteger contra vírus

Embora muitos Firewalls façam o *scan* de todo o tráfego entrante para determinar se este pode passar para a rede interna, o *scan* é destinado principalmente aos endereços fonte e destino, bem como o protocolo utilizado, e não para os detalhes dos dados. Até mesmo com filtragem de pacote sofisticada ou software de *proxying*, a proteção de vírus em um Firewall não é muito prática. Há muitos tipos de vírus e muitos modos que um vírus pode se esconder dentro de dados.

Detectar um vírus em um pacote aleatório de informações que passa pelo Firewall é muito complexo, este requer:

- Reconhecer que este pacote é parte de um programa;
- Determinar como o programa deveria parecer;
- Determinar que as mudanças ocorrem em função de vírus.

Até mesmo o primeiro destes é um desafio. A maioria dos Firewalls está protegendo máquinas de vários tipos com formatos de arquivos executáveis diferentes. Um programa pode ser um executável compilado ou um *script*. Além disso, a maioria dos programas é empacotado para transporte, e estão freqüentemente comprimidos.

Por estas razões, usuários podem acabar trazendo vírus para a rede interna, não importando o nível de segurança do Firewall. Mesmo que fosse possível implementar um Firewall que pudesse bloquear a entrada de vírus, o problema de vírus ainda não teria sido solucionado. Arquivos trazidos ao computador através de conexões discadas ou mesmo através de disquetes ainda seriam uma ameaça.

A maneira mais prática de lidar com o problema de vírus é a proteção baseada em host, com controle centralizado em um servidor antivírus. Outra medida de igual importância é o treinamento do usuário em conscientização sobre as questões de segurança. De uma forma geral o Firewall atua sobre os aspectos de protocolo do tráfego (inspeção de cabeçalho) mas não tem mecanismos para lidar com a informação que é carregado pelo tráfego.

3.3. ***Packet Filter*ing (Filtragem de Pacotes)**

Como um primeiro passo ao se implementar um Firewall em uma rede de computadores, é fundamental que se conheça os detalhes dos protocolos de comunicação utilizados. Na Internet, a atenção deve ser voltada aos protocolos IP, TCP, ICMP e UDP. Estes são os principais protocolos a nível de rede e transporte (Modelo OSI) que são considerados e examinados ao se estabelecer regras de filtragem em um *packet filter* para a Internet. Este mecanismo de filtragem a nível de roteador possibilita que se controle o tipo de tráfego de rede que pode existir em qualquer segmento de rede; consequentemente, pode-se controlar o tipo de serviços que podem existir no segmento de rede. Serviços que comprometem a segurança da rede podem, portanto, ser restringidos.

Com o exposto acima, fica evidente que um *packet filter* não se encarrega de examinar nenhum protocolo de nível superior ao nível de transporte, como por exemplo

o nível de aplicação que fica como tarefa dos *application gateways* (*proxy servers*). Portanto, qualquer falha de segurança a nível de aplicação não pode ser evitada utilizando somente um *packet filter*.

O componente que realiza a filtragem de pacotes geralmente é um roteador dedicado, mas também pode ser um host de uso geral configurado como roteador, e recebe a denominação de *screening router* (figura 3.1.). Há ferramentas freeware disponíveis na Internet para se configurar um simples PC como um roteador com recursos de filtragem de pacotes, consistindo em uma alternativa de baixo custo. A parte prática deste trabalho, no Capítulo 5 descreve exatamente isto. Deve-se ressaltar que o processo de filtragem de pacotes acarreta num overhead ao sistema; portanto, para uma situação de alto tráfego é necessário que se utilize um roteador com uma velocidade de processamento compatível com as necessidades.
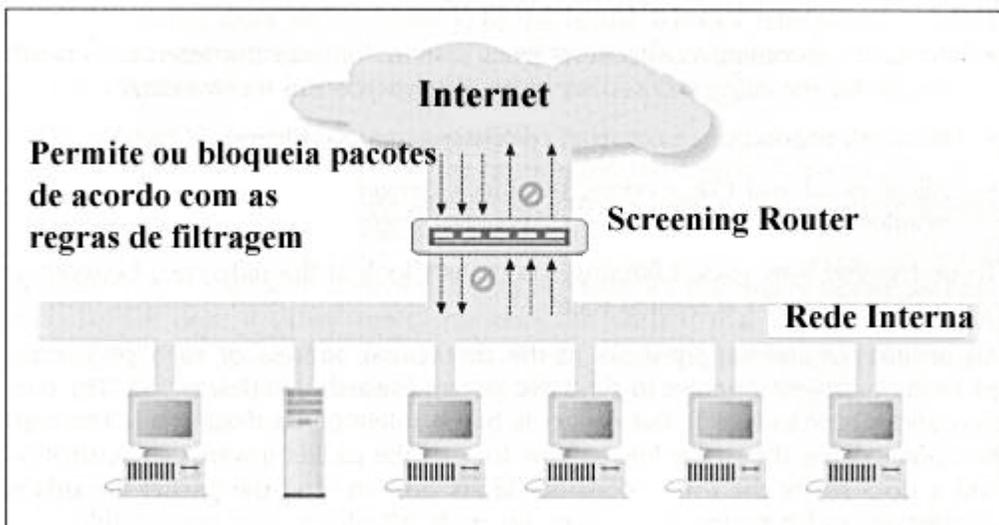
Figura 3.2: Atuação de um *Screening Router*

Frisando que a filtragem dos pacotes não considera protocolos acima do nível de transporte, não é tomada nenhuma decisão baseada no conteúdo dos pacotes; ou seja, nos dados dos pacotes propriamente ditos. A filtragem que a maioria *dos screening routers* realizam são baseadas nas seguintes informações:

- Endereço IP fonte;

- Endereço IP destino;
- Protocolo: Se o pacote é TCP, UDP ou ICMP;
- Portas TCP ou UDP fontes;
- Portas TCP ou UDP destino;
- Tipo de mensagem ICMP (se for o caso).

No protocolo TCP existe um flag denominado ACK que é utilizado para confirmação de pacotes e também pode ser utilizado para detectar se o pacote é o primeiro de uma solicitação de conexão. Quando o flag não estiver setado significa que o pacote se refere a uma solicitação de conexão e, caso contrário, o pacote corresponde a alguma conexão já existente (Figura 3.3.). Desta forma, o *packet filter* pode bloquear um serviço inbound (de fora para dentro; ou seja, o servidor está na rede interna) apenas não permitindo o fluxo de pacotes com o ACK setado destinado a um servidor interno associado a port (por exemplo, a port 23 do telnet) do serviço bloqueado. Em protocolos não orientados a conexão, por exemplo o protocolo UDP, não é possível tomar nenhuma decisão deste tipo; ou seja, nestes protocolos, nunca se sabe se o pacote que está chegando é o primeiro que o servidor está recebendo. Para fazer uma filtragem correta dos pacotes, é importante saber se o protocolo é bidirecional (pacotes fluem nos dois sentidos, cliente para servidor e vice-versa) ou unidirecional. Não se pode confundir serviços inbound (a rede interna provendo algum serviço) e serviços outbound (o cliente está na rede interna e o servidor na Internet) com pacotes inbound (pacotes que chegam na rede interna) e pacotes outbound (pacotes que saem da rede interna); ou seja, ambos os serviços apresentam pacotes inbound e outbound caso o protocolo seja bidirecional.
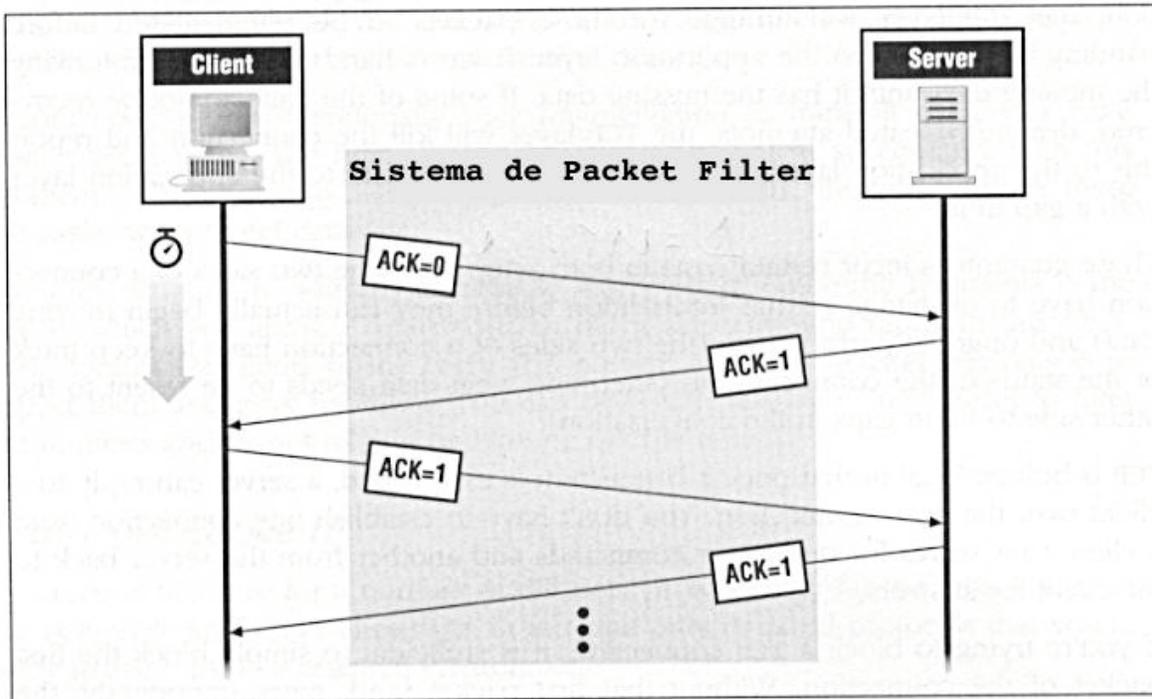
Figura 3.3: bit ACK no protocolo TCP

É importante que o roteador tenha facilidades de filtragem por interfaces de rede. Ou seja, todas as interfaces disponíveis no roteador são submetidas às regras de filtragem, possibilitando que as regras sejam aplicadas considerando as seguintes informações:

- A interface na qual o pacote chega;
- A interface pela qual o pacote sai.

O IP *Spoofing* (Figura 3.4.) é um ataque que pode ser evitado com a aplicação do recurso exposto acima. Neste ataque o intruso tenta se passar como um host interno (um host considerado confiável) utilizando o endereço IP deste como o endereço de origem. Se a filtragem é realizada por interface em ambos os sentidos, este ataque não funciona porque jamais um pacote pode chegar do mundo externo (Internet) tendo como endereço fonte o endereço de uma máquina que está na rede interna; ou seja, só poderia chegar naquela interface no outro sentido.
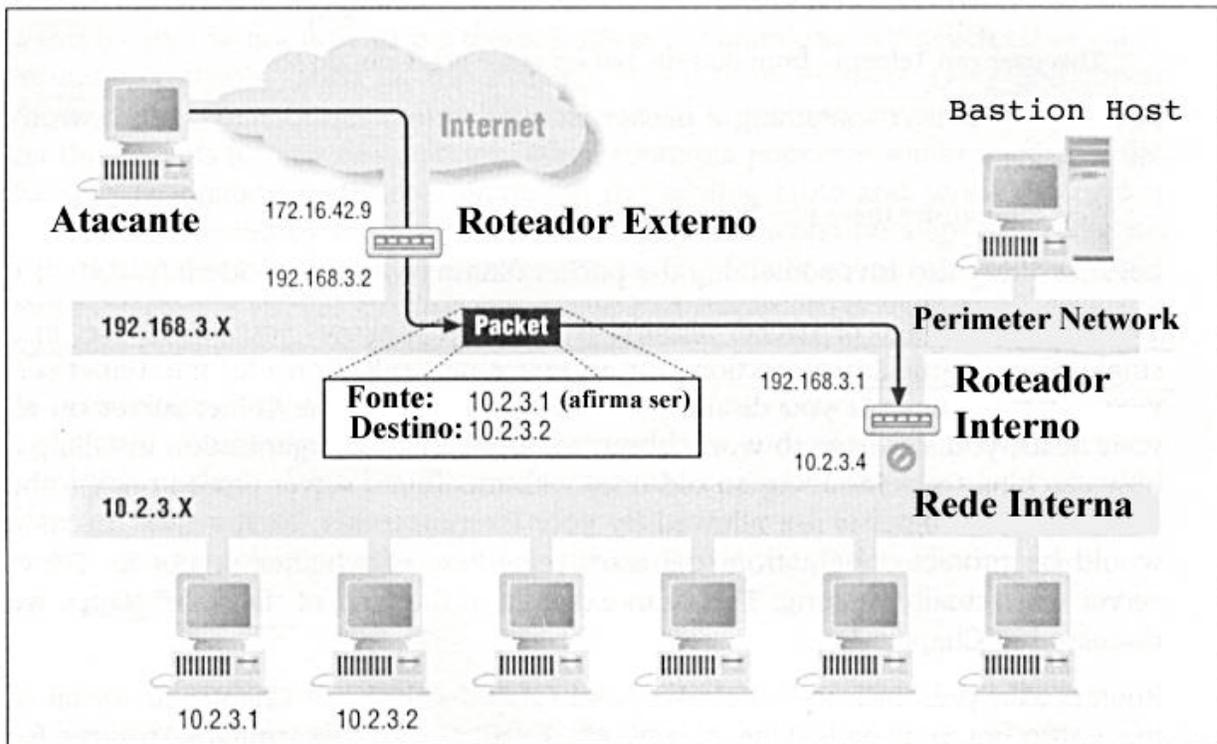
Figura 3.4: Ataque do tipo IP *spoofing*

Eis alguns exemplos de regras de filtragem que poderiam ser aplicadas em um *screening router*:

- Bloquear todas as solicitações de conexão de hosts da rede externa com a sub-rede "X.X.8" (conectada em alguma interface do roteador), exceto conexões SMTP (Porta TCP número 25);
- Bloquear todas as conexões para e de certos sites considerados não confiáveis;
- Desabilitar source routing (roteamento de e para a máquina destino especificado no próprio pacote);
- Bloquear os serviços considerados inseguros tais como Xwindows, RPC, NFS, TFTP, SNMP, NIS, etc.

A sintaxe dessas regras de filtragem depende do produto (roteador ou Firewall) utilizado, porque atualmente não existe um padrão de sintaxe. É aconselhável montar

uma tabela com as possibilidades de pacotes para cada serviço a ser provido. Veja um exemplo na TABELA 3.1 [15].

Direction	Source Addr.	Dest. Addr.	Protocol	Source Port	Dest. Port	ACK Set	Notes
In	Ext	Int	UDP	>1023	53	[a]	Incoming query via UDP, client to server
Out	Int	Ext	UDP	53	>1023	[a]	Answer to incoming UDP query, server to client
In	Ext	Int	TCP	>1023	53	[b]	Incoming query via TCP, client to server
Out	Int	Ext	TCP	53	>1023	Yes	Answer to incoming TCP query, server to client
Out	Int	Ext	UDP	>1023	53	[a]	Outgoing query via UDP, client to server
In	Ext	Int	UDP	53	>1023	[a]	Answer to outgoing UDP query, server to client
Out	Int	Ext	TCP	>1023	53	[a]	Outgoing query via TCP, client to server
In	Ext	Int	TCP	53	>1023	Yes	Answer to outgoing TCP query, server to client
In	Ext	Int	UDP	53	53	[a]	Query or response between two servers via UDP
Out	Int	Ext	UDP	53	53	[a]	Query or response between two servers via UDP
In	Ext	Int	TCP	>1023	53	[b]	Query from external server to internal server via TCP; also zone transfer request from external secondary server via TCP
Out	Int	Ext	TCP	53	>1023	Yes	Answer from internal server to external server via TCP; also zone transfer response to external secondary server via TCP
Out	Int	Ext	TCP	>1023	53	[b]	Query from internal server to external server via TCP
In	Ext	Int	TCP	53	>1023	Yes	Answer from external server to internal server via TCP

[a] UDP packets do not have ACK bits.

[b] ACK is not set on the first packet of this type (establishing connection) but will be set on the rest.

Tabela 3.1: Esquematização de Regras de filtragem (protocolo DNS).

Descrição dos campos da tabela:

- **Direction**: é a direção do pacote (in: entrando no roteador; out: saindo do roteador);
- **Source address**: é o endereço fonte;
- **Destination address**: é o endereço destino;
- **Protocol**: é o protocolo utilizado;
- **Source port**: é a porta fonte;
- **Destination port**: é a porta destino;
- **ACK set**: indica se o flag ACK está setado;
- **Notes**: apresenta um breve comentário sobre a regra.

3.3.1. Operações de um *Packet Filter*

Quase todos os dispositivos atuais de filtragem de pacotes operam da seguinte maneira [1]:

1. Os critérios de filtragem de pacotes devem ser armazenados para as portas do dispositivo de filtragem de pacotes. Os critérios de filtragem de pacotes são chamados "regras de filtragem de pacotes".
2. Quando o pacote chega em uma porta, os cabeçalhos do pacote são analizados. Muitos dispositivos examinam os campos somente nos cabeçalhos dos protocolos IP, TCP ou UDP.
3. As regras de filtragem são armazenadas em uma ordem específica. Cada regra é aplicada ao pacote na ordem em que as regras estão armazenadas.
4. Se uma regra bloqueia a transmissão ou recepção do pacote, o pacote é bloqueado.
5. Se uma regra permite a transmissão ou recepção do pacote, o pacote é aceito para prosseguir.
6. Se um pacote não satisfaz qualquer regra ele é bloqueado.

Pelas regras 4 e 5 fica evidente que a ordem das regras de filtragem é de fundamental importância. Uma ordenação incorreta das regras pode acarretar em bloqueio de serviços válidos e em permissão de serviços que deveriam ser negados. Da regra 6 segue a filosofia "O que não é expressamente permitido é proibido".

3.3.2. Vantagens e Desvantagens

Algumas vantagens dos *packet filter*s são:

- Pode ajudar a proteger toda uma rede, principalmente se este é o único roteador que conecta a rede interna à Internet;
- A filtragem de pacotes é transparente e não requer conhecimento nem cooperação dos usuários;
- Está disponível em muitos roteadores e/ou produtos específicos.

Algumas desvantagens são:

- As ferramentas de filtragem atualmente disponíveis não são perfeitas;
- Alguns protocolos não são bem adaptados para a filtragem;
- Algumas políticas não podem ser aplicadas somente com a filtragem de pacotes.

Quando se aplica alguma restrição em algum protocolo de mais alto nível, através de números de portas, espera-se que nada além do próprio serviço esteja associado àquela porta; entretanto, usuários internos mal intencionados podem subverter este tipo de controle colocando outro programa (desenvolvido por ele) associado a essa porta. Como citado anteriormente, um Firewall não é apropriado para se defender de ameaças internas.

3.3.3. Ações do Screening Router

O roteador encarregado da filtragem dos pacotes pode executar uma série de atividades que servem, entre outras coisas, para monitorar o sistema. Algumas atividades são:

- Realizar logs de acordo com a configuração especificada pelo administrador. Dessa forma, é possível analisar eventuais tentativas de ataque, bem como verificar a correta operação do sistema;
- Retorno de mensagens de erros ICMP: caso um pacote seja barrado existe a possibilidade de se enviar ao endereço fonte alguma mensagem com o código de erro ICMP do tipo *host unreachable* ou *host administratively unreachable*. Entretanto, tais mensagens, além de causar um overhead, podem fornecer algumas informações sobre o *packet filter* ao atacante, pois dessa forma ele poderia descobrir quais os protocolos que são barrados e quais estão disponíveis; portanto, recomenda-se que não se retorne nenhum código ICMP de erro para hosts na rede externa.

3.3.4. Riscos na filtragem

A filtragem por endereço fonte apresenta alguns riscos. Há dois tipos de ataques possíveis:

- *Source address*: o atacante forja o endereço fonte utilizando o endereço de uma máquina (externa ou interna) considerada confiável (trusted) pelo Firewall (Figura 3.3.). Este ataque pode ter sucesso principalmente quando o atacante não precisa capturar (ou seja, estar em um caminho entre o Firewall e o host forjado) nenhum pacote e, caso a máquina forjada seja interna, não houver mecanismos de filtragem que impeçam o ip *spoofing* (citado anteriormente); a resposta ao ataque poderia ser o

envio de alguma informação (por exemplo o arquivo passwd) via e-mail diretamente ao atacante;

- *Man in the middle*: além de forjar o endereço, nesse ataque o atacante deve estar no caminho entre o Firewall e o host confiável porque ele tem de capturar os pacotes que são, na realidade, enviados ao host confiável (daí a denominação do ataque).

Muitos desses ataques só funcionam quando o host confiável (aquele cujo endereço é utilizado pelo atacante) estiver fora de operação, porque assim que ele receber algum pacote que não esteja relacionado com nenhuma conexão que ele tenha iniciado ele solicitará que a conexão forjada seja encerrada. Existem várias formas de se evitar que o host confiável tome conhecimento da conexão forjada pelo atacante, eis alguns métodos:

- Confundindo o roteamento entre a máquina real (host confiável) e a máquina alvo;
- Utilizando um ataque onde somente a primeira resposta é requerida, de tal forma que o reset solicitado pela máquina real não importará;
- Inundando a máquina real com pacotes lixo (por exemplo, pacotes ICMP) enquanto o ataque ocorre, de forma que a máquina real ficará ocupada tentando processar os pacotes lixo que ela recebe;
- Utilizando *source routing*.

A filtragem baseada na porta de origem apresenta um problema semelhante àquele da filtragem pelo endereço fonte. Assume-se que a uma determinada port um determinado serviço esteja associado, mas nada impede (como citado anteriormente) que alguém com os devidos direitos (por exemplo, root no Unix) substitua o servidor por outro. Para evitar este tipo de ataque, deve-se garantir que o servidor seja confiável e execute somente o permitido; impedindo, de outra forma, que o cliente devidamente modificado possa solicitar alguma facilidade que comprometa o servidor. Portanto, é

fundamental que tanto o servidor como também os clientes utilizados não sejam passíveis de serem alterados indevidamente por pessoas mal intencionadas.

3.3.5. Características desejáveis em um screening router

Eis algumas características altamente desejáveis a fim de que se possa realizar uma filtragem de pacotes bem apurada:

- Ter uma boa performance na filtragem dos pacotes: um *overhead* aceitável de acordo com as necessidades;
- Pode ser um roteador dedicado ou um computador de propósito geral executando algum sistema de roteamento;
- Permitir uma especificação de regras de forma simples;
- Permitir regras baseadas em qualquer cabeçalho ou critério meta-*packet* (por exemplo, em qual interface o pacote chegou ou está saindo);
- Aplicar as regras na ordem especificada;
- Aplicar as regras separadamente para pacotes que chegam e partem em e de cada interface de rede;
- Registrar informações sobre pacotes aceitos e rejeitados;
- Ter capacidade de teste e validação.

3.4. Conclusão

Neste capítulo demonstrou-se a utilização do Firewall em suas mais diversificadas aplicações. Abordou-se ainda uma série de recursos, deficiências e limitações, bem como características que podem ser encontradas em qualquer sistema de segurança. Mais adiante verifica-se a utilização do *Packet Filtering*, seu comportamento diante do recebimento e envio dos pacotes, vantagens, desvantagens e riscos.

Capítulo 4 – Desenvolvimento dos Procedimentos de Segurança

O modelo adotado para os procedimentos de segurança foi desenvolvido em três fases. A primeira consistiu da aplicação de um questionário, junto ao pessoal do Laboratório de Bioinformática, de um questionário, com o objetivo de fazer uma avaliação preliminar. O questionário foi baseado no modelo encontrado no capítulo 46 do livro "*Computer Security Handbook* "[10].

A segunda fase consistiu na descrição da situação atual do Laboratório de Bioinformática, baseada nos dados obtidos da avaliação preliminar tendo sido feita uma descrição dos equipamentos existentes no Laboratório de Bioinformática. Alguns dados referentes ao Laboratório de Biologia Molecular (BIOMOL), o qual engloba o Laboratório de Bioinformática (BIOINFO), foram também levantados, pois constituem informações relevantes para a o desenvolvimento do modelo de segurança deste último.

A terceira fase corresponde aos procedimentos desenvolvidos a partir dos dados coletados e das demandas existentes na Bioinformática. Apesar de alguns dos procedimentos já estarem em vigor no momento de sua descrição nesta fase, fica importante sua citação para que futuros administradores de rede e usuários possam saber dos procedimentos existentes e também daqueles cuja implementação se faz necessária.

O desenvolvimento dos procedimentos foi baseado em dois modelos existentes:

- RFC2196 (*Site Security Handbook*) [3];
- *IT Baseline Protection Manual* [4];

Estes dois modelos foram adotados como base por duas razões. Primeiro porque são modelos abrangentes, possuindo arcabouço teórico para auxiliar o desenvolvimento dos procedimentos necessários. Segundo porque são gratuitos, diferentemente do ISO (*Information Security Officer´s Manual*) [2], que apesar de ser abrangente e detalhado, deve ser adquirido.

4.1. Avaliação Preliminar (Fase I)

A meta da avaliação preliminar é perguntar às pessoas que trabalham com os recursos de informação, através de um questionário individual (anexo 1), o que elas acreditam ser suas maiores necessidades de segurança. Mesmo que elas não tenham o nível de consciência em segurança esperado, na prática os usuários têm intuições valiosas que transcendem a teoria e as generalizações.

Os seguintes assuntos devem fazer parte do estudo preliminar (sua abrangência está descrita entre parênteses):

- Introdução ao estudo;
- Estado da política atual (BIOMOL e BIOINFO);
- Classificação de Dados (BIOINFO);
- Sistemas Sensíveis (BIOINFO);
- Sistemas Críticos (BIOINFO);
- Autenticidade (BIOINFO);
- Exposição (BIOINFO);
- Recursos humanos, gerenciamento e cuidados com a segurança dos empregados (BIOMOL e BIOINFO);
- Segurança Física (BIOMOL e BIOINFO);
- Segurança das operações com computadores (BIOINFO);
- Controle de acesso a dados (BIOINFO);
- Segurança da rede e comunicações (BIOINFO);
- Medidas Antivírus (BIOMOL e BIOINFO);
- Backups, arquivos e destruição de dados (BIOINFO);

As respostas ao questionário encontram-se no anexo 4.

4.2. Descrição da situação atual (Fase II)

Esta fase tem como objetivo fazer uma descrição do panorama atual dentro do Laboratório de Bioinformática (BIOINFO), no que diz respeito a cada um dos tópicos do questionário aplicados aos seus usuários, além de uma descrição dos equipamentos existentes. Existem tópicos cuja descrição também estará relacionada ao Laboratório de Biologia Molecular.

4.2.1. Estado da política atual

Em função das respostas dos questionários aplicados (anexo 4), pode-se constatar que o Laboratório de Biologia Molecular da UnB (BIOMOL) não possuía nenhuma política de segurança em funcionamento. Sendo assim, não havia disponibilidade de acesso a esta por meio de documentos, nem tampouco ninguém era responsável por mantê-las. Em termos de chefia, o pessoal da coordenação do BIOINFO são subordinados ao Professor Marcelo Brígido.

Quanto ao monitoramento dos padrões de uso do BIOINFO, estes são monitorados por conta de cada indivíduo que usa o local, ou seja, não existe nenhuma pessoa responsável pelo controle do uso do laboratório.

4.2.2. Classificação de Dados

Quanto à classificação dos dados em níveis de segurança, esta classificação existe em nível informal, ou seja, existem dados que devem possuir maior segurança, como é o caso das seqüências de dados enviados por outros pesquisadores, porém não existe nenhuma regra nem documentos explicitando o nível de confidencialidade de cada informação tratada.

Em geral, os entrevistados acreditam ser importante classificar os dados em níveis de segurança, pois os dados referentes ao trabalho de pesquisa requerem alta confidencialidade.

No momento, esta classificação informal existe por demanda, ou seja, os dados são classificados como de alta confidencialidade ou não em função do andamento do projeto.

4.2.3. Sistemas Sensíveis

Os entrevistados estão conscientes da necessidade de proteção contra revelação não autorizada de informações, documentos ou sistemas existentes no laboratório.

A proteção das informações sensíveis por parte dos usuários é feita através de login com senha. No caso de outra pessoa do laboratório querer lidar com informações sensíveis de maneira anônima, a forma possível seria utilizando outra senha de usuário. Outra maneira possível seria conhecendo o endereço completo da página Web desejada, pois não existe verificação de sessão.

Quanto à revelação de informações sensíveis do laboratório (BIOINFO), os entrevistados afirmaram que não conheciam a ocorrência deste fato. Porém, relataram que já ocorreram eventos desta natureza em outro laboratório, demonstrando preocupação quanto à possibilidade de ocorrer este evento no laboratório. Os eventos ocorridos previamente no laboratório foram problemas com vírus e invasão de servidor Web.

No que se refere às sugestões dos entrevistados, pode-se ressaltar o desenvolvimento de um sistema de autenticação via Web, para que os acessos às páginas sensíveis ocorresse com verificação de sessão. Outra sugestão foi a implementação da segurança do SGBD, para filtrar o acesso ao banco de dados.

4.2.4. Sistemas Críticos

Sobre as informações que necessitam de atenção especial quanto à disponibilidade e exatidão, constatou-se que as informações contidas no banco de dados devem ser protegidas quanto à destruição ou modificação não autorizada.

A precaução dos entrevistados quanto à guarda de informações críticas do laboratório corresponde à restrição de login dos usuários.

4.2.5. Autenticidade

No BIOINFO, os entrevistados não identificaram nenhum caso de uso de outra identidade para envio de e-mail, faxes ou cartas. Pode-se constatar também a inexistência de assinatura digital.

Quanto ao uso de cópias de sistemas proprietários, verificou-se o uso destas, sendo que os entrevistados não demonstraram haver problema nisso. Como justificativa, foi identificada a necessidade de uso de ferramentas de software utilizadas em determinado sistema proprietário.

4.2.6. Exposição

Segundo os entrevistados, entre as piores conseqüências que poderiam ocorrer se houvesse a divulgação de dados mais sensíveis do laboratório, pôde-se identificar:

- Perda da autoria do trabalho;
- Outros laboratórios concorrentes poderiam utilizar a informação para saber o nível de desenvolvimento da pesquisa ou mesmo utilizar os dados do trabalho para benefício próprio;
- Desenvolvimento de remédios e monopólio da patente por parte de laboratórios interessados.

Dentre as piores conseqüências provenientes de alterações não autorizadas ou acidentais de informações críticas, pôde-se destacar a inconsistência dos dados da pesquisa, que pode levar a perda de todo o trabalho desenvolvido.

4.2.7. Recursos humanos, gerenciamento e cuidados com a segurança do pessoal

Os procedimentos de segurança (do BIOMOL e BIOINFO), por existirem apenas de maneira informal, não podem ser acessados pelos seus membros, sendo que os usuários nunca assinaram nenhum termo de compromisso ou outro documento concordando com os procedimentos de segurança do BIOMOL. Não existe nenhuma pessoa responsável pela monitoração da concordância com os procedimentos de segurança, bem como seus membros nunca receberam nenhum treinamento no uso destes procedimentos. De modo geral, os entrevistados acreditam que seja uma de suas responsabilidades oficiais a proteção da informação do laboratório.

4.2.8. Segurança Física

Sobre a segurança física do BIOMOL, pôde-se constatar que a identificação dos seus membros não é feita quando da entrada no recinto (os visitantes também não usam crachás). Os sistemas de controle de acesso aos usuários são portas com tranca, porém, caso um estranho solicite que um usuário segure a porta a fim de que este possa entrar também, o usuário (por relato dos entrevistados) segura a porta e garante o acesso ao estranho no recinto. Em períodos onde ninguém está no recinto, o laboratório permanece com suas portas fechadas.

No caso de um dos usuários do BIOMOL identificar um estranho na área interna, nenhum questionamento ou solicitação à segurança seria feito. Em caso de alarme de incêndio, os entrevistados responderam que a medida a ser tomada seria trancar o laboratório e evacuar a área. Estes demonstraram desconhecimento quanto à localização do extintor de incêndio mais próximo. Os entrevistados disseram não possuir nenhum treinamento para enfrentar situações de emergência (bem como evacuação de área).

Em casos de emergência médica ou de segurança, existe um número para o qual os usuários podem discar.

Como medidas de melhoria da segurança física do BIOMOL, os entrevistados apontaram a utilização de crachás e a instalação de grades internas nos aparelhos de

ar condicionado, em função destes, quando retirados, permitirem acesso à parte externa do laboratório.

4.2.9. Segurança das operações com computadores

A partir do lançamento de uma nova atualização do sistema operacional em uso, o mesmo sinaliza nos computadores do laboratório (BIOINFO) que o sistema precisa ser atualizado, bem como envia e-mail ao administrador avisando da atualização. A atualização é primeiramente feita em uma máquina, e caso esta esteja funcionando corretamente após avaliação, os outros computadores do laboratório são atualizados. O relato de problemas, por parte dos usuários, é feito de maneira direta com a pessoa envolvida, não existindo nenhum sistema automatizado para recepção de problemas.

As pessoas externas ao BIOINFO não podem acessar os computadores deste, sendo a única possibilidade de acesso a obtenção de uma conta de usuário cadastrado e ativo.

Pessoas contratadas, incluindo técnicos de reparo, não podem circular pela área do BIOINFO sem estarem acompanhados. Da mesma forma, o pessoal da limpeza só pode acessar esta área com a presença de algum membro do BIOINFO.

O intervalo de tempo entre a aquisição de um componente do sistema e a colocação de seu número de patrimônio é grande, sendo assim possível que um monitor seja trocado de estação de trabalho sem que isto seja identificado.

Na área do laboratório de Bioinformática existe um sistema de permanência de energia (*NO-BREAK*, com aproximadamente 30 minutos de autonomia), que no momento abrange as *CPUs*, os monitores, o *Switch* e o dispositivo de backup deste. Este dispositivo não abrange o ar condicionado. Não existem registros dos momentos onde o sistema ficou fora do ar. Em relatos dos entrevistados, pôde-se identificar que ocorreram dois eventos desta natureza nos últimos três meses.

A utilização de recursos de largura de banda e de sistema não é monitorada por nenhum dispositivo. Somente a utilização da CPU dos computadores individuais pode ser monitorada atualmente.

Dentre as melhorias em segurança de operações com computadores sugeridas pelos usuários, pode-se destacar a colocação de número de patrimônio nos equipamentos e a monitoração da rede.

4.2.10. Controle de acesso a dados

Os usuários do BIOINFO necessitam de identificação através de login com senha para acessar o projeto com a qual trabalham, sendo que suas identificações não são nem foram compartilhadas com outros usuários.

Existem limitações quanto à permissão de acesso às informações em função da senha. No trabalho, não é utilizada nenhuma forma de encriptação de dados.

De acordo com os entrevistados, os usuários não levam trabalho para casa, porém não existe nenhuma norma que impossibilite ou monitore a forma com que um membro do laboratório de Bioinformática leve trabalho para seu domicílio.

4.2.11. Segurança da rede e comunicações

De acordo com os entrevistados, não há conhecimento de ninguém que viole as restrições de uso do sistema, bem como não é do conhecimento destes que alguém veja pornografia dentro do trabalho (infantil ou não), bem como materiais racistas.

Não existem diagramas de rede atualizados, porém, existe a possibilidade de produzi-lo por demanda, segundo o administrador de rede. O administrador de rede (BIOINFO) tem conhecimento de todos os serviços que estão rodando em sistemas conectados à Internet, sendo todos eles necessários segundo ele.

Sobre a atualização de *patches*, o próprio sistema avisa (ao ser inicializado ou por e-mail) ao administrador da necessidade de aplicação.

Na arquitetura de segurança do sistema, existe um Firewall incluído (*IPTables*, rodando em Linux RedHat 7.3), o que possui suas regras instanciadas em função dos serviços que estão sendo executados. O sistema não possui nenhum IDS instalado.

No BIOINFO, a liberação de novas senhas depende de autorização superior. Não existe controle de acesso remoto centralizado no sistema. Os usuários não aplicam

assinatura digital às suas comunicações. Em função da existência do Firewall, o administrador ressaltou que o servidor Web está protegido contra invasão, sendo que a informação sensível do sistema encontra-se dentro do servidor Web, e esta não está encriptada.

Em caso de vandalismo (pichamento de página), o tempo de restauração do backup do servidor Web fica em 10 minutos, segundo o administrador.

Em caso de demissão de funcionário ou de suspensão da autorização do acesso ao BIOINFO, o administrador só tem conhecimento do fato caso Marcelo Brígido informe diretamente. Não existe nenhuma forma de aviso formal e geral aos usuários do ocorrido.

4.2.12. Medidas Antivírus

O uso de produtos antivírus em estações de trabalho do BIOMOL ocorre de maneira independente, ou seja, cada um fica responsável pela compra (ou uso de cópia não autorizada), instalação e manutenção do software de antivírus. Nem todos os usuários possuem produtos desta natureza, e aqueles que possuem nem sempre estão com este atualizado. Segundo relatos, problemas com anexos de arquivos infectados em mensagens são freqüentes.

4.2.13. Backups, arquivos e destruição de dados

A freqüência da ocorrência de backup dos arquivos do sistema é feita a critério do administrador. Não existe uma periodicidade para a realização do backup, este é feito principalmente quando ocorre alguma modificação importante dentro do sistema.

A mídia de backup é armazenada dentro da própria unidade de backup, sendo que não existem cópias fora do laboratório. Como só existe uma mídia de backup, esta é a mídia utilizada em caso de necessidade de restauração de um arquivo específico.

Como o backup é feito sob demanda de atualização do sistema, o backup é mantido até que nova atualização do sistema ocorra e então é substituído por outro mais atualizado.

Não existe modo de prevenção ao acesso à mídia de *backup*, bem como não há *backup* de documentos em papel nem procedimentos de descarte de fitas que ultrapassaram o ciclo de vida útil.

4.2.14. Descrição do Hardware existente no Laboratório de Bioinformática

Estações de trabalho

Dentro da sala de Bioinformática do laboratório de Biologia Molecular, estão os modelos de estações de trabalho Dell, descritos nas tabelas 4.1 e 4.2.

Dell Optiplex™ GX150 SD	
Item	Configuração
Processador	Intel Pentium III de 1 GHz com chipset 815e
Memória	256 MB SDRAM
Disco rígido	20 GB
Monitor	17”
Placa de vídeo	Intel 3D AGP Graphics DVMT
Placa de áudio	AC97 integrada
Alto-falantes	Nenhum
Placa de rede	3com 10/100 integrada
Unidade óptica	CD-ROM 48X
Unidade de disquete	3.5” 1.44 MB
Gabinete	Desktop
Teclado	QuietKey em português (ABNT II)
Mouse	Microsoft Intellimouse com mousepad
Sistema operacional	Microsoft Windows 98 em português (OptiPlex não tem opção do Linux)
Aplicativo	Gerenciador de rede “Dell OpenManage”
Garantia	3 anos no local e por telefone “lifetime”
Quantidade de peças	4 computadores

Tabela 4.1: Descrição das estações de trabalho Dell Optiplex™ GX150 SD

Dell Precision™ 530	
Item	Configuração
Processador	Biprocessado (dois processadores com a especificação abaixo): Intel Xeon de 1,5 GHz com chipset 860 / FSB 400 MHz 264 KB de memória cache
Memória	512 MB RDRAM PC800
Disco rígido	2 discos de 20 GB EIDE ULTRA ATA-100
Placa de vídeo	4X AGP nVIDIA Quadro 2 EX com 32MB
Monitor	19”
Placa de áudio	AC97 integrada
Alto-falantes	Não solicitados
Placa de rede	3com 10/100 integrada
Unidade óptica 1	CD-RW 16X (não disponível opção sem CD)
Unidade óptica 2	Iomega Zip 250 MB
Unidade de disquete	3.5” 1.44 MB
Gabinete	Torre
Teclado	QuietKey em inglês
Mouse	LogitechClub 3 botões
Sistema operacional	Linux 7.1 Red Hat Service + Sound
Aplicativo	Gerenciador de rede “Dell OpenManage”
Garantia	3 anos no local e por telefone “lifetime”
Quantidade de peças	2 computadores

Tabela 4.2: Descrição das estações de trabalho Dell Precision™ 530

Servidores

Dentro do Laboratório de Bioinformática, existem os modelos de servidores Dell descritos nas tabelas 4.3 e 4.4.

Dell PowerEdge 1400SC	
Item	Configuração
Processador	1 Processador Pentium III de 1.26GHz com 512KB de memória cache, expansível a 2048
Memória	512 MB de memória RAM (2x256)
Disco rígido	01 disco rígido de 36GB SCSI Ultra3 de 10.000 rpm
Monitor	15”
Alto-falantes	Não solicitados
Placa de rede	2 Placas de rede BROADCOM NetXtreme 10/100/1000 CAT 5
Unidade óptica 1	CD-ROM de 48X
Unidade de disquete	3.5” 1.44 MB
Gabinete	Torre
Teclado	QuietKey em inglês
Mouse	Logitech 2 botões
Sistema operacional	Inexistente
Garantia	3 anos no local e por telefone “lifetime”
Quantidade de peças	1 computador

Tabela 4.3: Descrição do servidor Dell PowerEdge 1400SC

Dell PowerEdge 6400	
Item	Configuração
Processador	4 Processadores Pentium III Xeon de 700MHz com 2MB de memória cache
Memória	2 GB de memória RAM (4x512)
Disco rígido	- 02 discos rígidos de 73GB SCSI Ultra3 de 10.000 rpm - 02 discos rígidos de 18GB SCSI Ultra3 de 15.000 rpm
Monitor	17”
Alto-falantes	Não solicitados
Controladora	Controladora de array com 2 canais SCSI Ultra3 e 128MB de memória cache com bateria
Placa de rede	1 Placa de rede Intel 10/100 Integrada 2 Placas de rede intel 10/100 PCI Dual Port
Unidade óptica	- 01 Unidade de CD-ROM de 48x - 01 Unidade de CD-RW 12X8X32
Unidade de disquete	3.5” 1.44 MB
Gabinete	Torre
Teclado	QuietKey em inglês
Mouse	Logitech 2 botões
Sistema operacional	Inexistente
Ventilação	Ventiladores redundantes e hot-pluggable
Energia	Fontes de alimentação redundantes e hot-pluggable
Garantia	3 anos no local e por telefone “lifetime”
Quantidade de peças	1 computador

Tabela 4.4: Descrição do servidor Dell PowerEdge 6400

Switch

Extreme Networks Summit 24e2
Especificações
Backplane não blocante de 8.8 Gbps sobre 6.6 milhões de pacotes por segundo
24 portas Ethernet
2 portas Gigabit Ethernet ativas em duas opções de versões
VLANS 64 IEEE 802.1Q
Agregação de link compatível com IEEE 802.1ad
Qualidade de serviço 802.1p
Gerenciamento local ou remoto (via telnet)

Tabela 4.5: Descrição do Switch Extreme Networks Summit 24e2.

Impressora

Hp Laserjet 2100	
Característica	Descrição
Tipo	Impressora Laser
Tecnologia	Eletrostática, Laser
Resolução	1200 x 1200 dpi
Compatibilidade	IBM / MAC / UNIC
Velocidade de Impressão	10 ppm
Tamanho máximo de papel	8.5” (216 mm) x 14”
Capacidade de papel	250 folhas
Capacidade de memória	4MB (mín) / 52MB (máx)
Temperatura de Operação	10º - 30ºC
Umidade de Operação	20 – 80%

Tabela 4.6: Descrição da impressora Hp Laserjet 2100

4.3. Procedimentos de Segurança (Fase III)

4.3.1. Introdução

4.3.1.1. Propósito do trabalho

O propósito principal da criação de procedimentos de segurança é identificar as vulnerabilidades de segurança do BIOINFO (ou mesmo BIOMOL, quando se aplicar), bem como descrever os motivos pelos quais estas vulnerabilidades foram identificadas e finalmente especificar as medidas necessárias a fim de minimizá-las.

4.3.1.2. A quem se destina

As medidas necessárias à minimização das vulnerabilidades de segurança tem como alvo os administradores de rede e usuários do BIOINFO, como também os responsáveis pela administração física do local (BIOMOL).

4.3.1.3. Como estão distribuídos os procedimentos

A partir dos dados obtidos na Fase 2 (Descrição da situação atual), a sua distribuição dentro dos Procedimentos de Segurança ocorreu da maneira apresentada na tabela 4.7.

<table>
<tr><th>FASE 2</th><th colspan="2">FASE 3</th></tr>
<tr><td>4.2.2. Classificação de dados</td><td colspan="2">4.3.4.2. Classificação de informação</td></tr>
<tr><td>4.2.3. Sistemas sensíveis</td><td colspan="2" rowspan="4">4.3.4.3. Sistemas críticos e controle de acesso a dados</td></tr>
<tr><td>4.2.4. Sistemas críticos</td></tr>
<tr><td>4.2.5. Autenticidade</td></tr>
<tr><td>4.2.6. Exposição</td></tr>
<tr><td>4.2.7.Recursos Humanos, gerenciamento e cuidados com a segurança do pessoal</td><td colspan="2">4.3.4.1. Recursos Humanos, gerenciamento e cuidados com a segurança do pessoal</td></tr>
<tr><td>4.2.8 Segurança física</td><td colspan="2">4.3.3.1. Segurança física</td></tr>
<tr><td>4.2.9. Segurança das operações com Computadores</td><td colspan="2">4.3.4.6. Operações com computadores</td></tr>
<tr><td rowspan="3">4.2.11. Segurança de rede e comunicações</td><td rowspan="3">4.3.2. Comunicações</td><td>4.3.2.1. Firewall</td></tr>
<tr><td>4.3.2.2. IDS</td></tr>
<tr><td>4.3.2.3. Servidor Web e acesso remoto</td></tr>
<tr><td>4.2.12. Medidas antivírus</td><td colspan="2">4.3.4.4. Proteção antivírus</td></tr>
<tr><td>4.2.13. Backups, arquivos e destruição de dados</td><td colspan="2">4.3.4.5. Procedimentos de Backup</td></tr>
</table>

Tabela 4.7: Distribuição dos Procedimentos a partir dos dados obtidos na Fase II.

4.3.2. Comunicações

4.3.2.1. Firewall

Descrição

O Firewall tornou-se tanto o conceito como a realização da proteção e segurança da rede e Internet. Pela sua rápida aceitação e evolução, o Firewall tornou-se a

tecnologia de segurança mais visível nas empresas e nos outros locais de sua utilização.

Firewall, como mecanismo de segurança de redes, tem fornecido proteção à conectividade de um determinado local com a rede externa, mais visivelmente a Internet [10].

Um Firewall é um dos mecanismos usados no controle de acesso a uma rede, com a finalidade de protegê-la. Um Firewall age como um *Gateway* através do qual todo o tráfego entra e sai. Firewalls ajudam a colocar limitações na quantidade e no tipo de comunicação que trafega entre a rede protegida e uma outra rede, por exemplo, a Internet e outra parte da rede local.

Um Firewall geralmente é um modo de construir uma parede entre uma parte de uma rede (a rede interna do laboratório) e a parte externa (como a Internet). A característica peculiar sobre esta parede é que devem existir modos específicos para que um tráfego com características particulares passe através de suas portas monitoradas (*Gateways*). A parte difícil está no estabelecimento dos critérios pelos quais a passagem dos pacotes pelas portas é permitida ou negada (regras de filtragem) [6].

Motivação

No laboratório, apesar da existência de um Firewall (*IPTables*, instalado em um Linux RedHat 7.3), já ocorreram casos de invasão no servidor Web e modificação de páginas.

Desta forma, existe a necessidade de instalação de um Firewall, com um conjunto de regras compatíveis às necessidades de segurança e aos serviços que devem rodar no sistema, que tem como objetivos:

- Proteger o servidor de Banco de Dados de seqüências biológicas de tráfego hostil, visando manter a integridade do mesmo.
- Proteger as estações da rede interna do Laboratório de Bioinformática, de tráfego hostil.
- Ser uma solução sem ônus e efetiva.

Medidas

- Instalação de um servidor de Firewall, com as seguintes características:
  - ➢ Sistema Operacional OpenBSD (última versão);
  - ➢ Filtragem de Pacotes através do *Packet Filter* (sistema de filtragem de pacotes padrão do OpenBSD, a partir da versão 3.0);
  - ➢ Três interfaces de rede: Uma para a rede externa, com endereço válido e outras duas subredes internas inválidas, uma para as estações e outra para o servidor Web.
  - ➢ Tradução do endereço de rede inválido (NAT) do servidor Web, a fim de que ocorra a comunicação entre este e computadores da rede externa.
  - ➢ Criação de um conjunto de regras referentes à realização dos serviços essenciais.
- Abrangência – BIOINFO.

4.3.2.2. Sistema de Detecção de Intrusão (IDS)

Descrição

Quando perguntados sobre como lidar com a segurança de redes de computadores, a maioria das pessoas menciona Firewalls. De fato, Firewalls foram os primeiros produtos de segurança de redes largamente utilizados.

Porém, apesar de ser efetivo, os Firewalls não são uma solução completa de segurança. Embora eles possam restringir o tráfego para o que os gerentes de rede desejam que seja permitido, eles não são capazes de prevenir ataques se o tráfego hostil passar pelo Firewall.

Os sistemas de detecção de intrusão (IDSs) são softwares ou hardwares que automatizam a monitoração de eventos que ocorrem internamente a um sistema computacional ou rede. Os IDSs não apenas coletam e sincronizam registros destes

eventos, mas também fazem uma análise dos mesmos procurando por sinais de violações de segurança [10].

Motivação

Apesar da existência de um Firewall, existe a necessidade de determinar o nível de ameaça a que uma rede está sujeita. Sistemas de Detecção de Intrusão baseados em rede freqüentemente realizam esta tarefa, realizando esta monitoração quando colocados entre o Firewall e a rede externa.

Os IDSs também são uma valiosa ferramenta de segurança para os sistemas, pois auxiliam a monitoração do tipo de tráfego que sai da rede interna. Assim como o Firewall, o IDS deve ser uma solução efetiva e sem ônus.

Medidas

- Instalação de um Sistema de Detecção de Intrusão com as seguintes características:
  - ➢ Utilização do Snort [7] como IDS padrão, em uma plataforma com OpenBSD como sistema operacional.
  - ➢ Localização do sensor externo ao Firewall do laboratório.
  - ➢ Utilização de resposta passiva, sendo que o IDS comunica os resultados do processo de detecção ao responsável, o qual deve então interpretar os resultados.
  - ➢ Criação de um conjunto de regras referentes à detecção de intrusão.
  - ➢ Utilização da interface de análise da base de dados de intrusão (ACID) [8], com conexão encriptada HTTPS (SSL / TLS), em servidor Apache.
- Abrangência – BIOINFO.

4.3.2.3. Servidor Web e Acesso Remoto

Descrição

Proteger um servidor Web significa garantir que o site e suas funcionalidades estejam disponíveis ininterruptamente durante o dia, todos os dias da semana. Esta proteção também significa que a informação trocada com o site deve ser precisa e segura (integridade).

A proteção do servidor Web reside na junção da tecnologia, da estratégia, da relação das pessoas que acessam as páginas e do gerenciamento do projeto. De maneira geral, a disponibilidade do servidor Web e sua integridade afetam diretamente o bom andamento de todo um projeto.

O acesso remoto é a capacidade de obter acesso a um computador ou uma rede a partir de uma distância remota. Nas corporações, o pessoal dos escritórios de filiais e as pessoas que estão viajando podem precisar de acesso à rede da corporação. Usuários domésticos fazem acesso remoto à Internet via um provedor (ISP). Conexões Dial-up, ADSL, ou por rádio feitas por computadores de mesa, computadores portáteis (laptops), ou palmtops são métodos comuns de acesso remoto [10].

Motivação

O acesso remoto aos sistemas do laboratório (no caso a página Web) e aos Banco de Dados é feito por redes externas, fora do controle direto do laboratório (como a Internet), o que constitui uma ameaça considerável.

Os dados transmitidos pelos usuários remotos são de alta confidencialidade, necessitando também como requisito de segurança a integridade. Existe também a necessidade dos usuários remotos realizarem um login com autenticação de ID e senha.

Medidas

- Em função da confidencialidade da natureza da informação processada pelo servidor Web, este deve suportar e ter implementado o Protocolo Seguro de

Transferência de Hipertexto (HTTPS – Hypertext transfer protocol secure), usando TCP (Transmission Control Protocol) porta 443.

- O servidor Web deve estar localizado internamente ao Firewall, em uma DMZ (Demilitarized Zone), região não militarizada localizada entre o Firewall e a rede externa. Nesta configuração, o Firewall possui uma interface ligada à rede externa (com endereço válido) e duas interfaces na rede interna (com endereços inválidos), uma para a rede interna e outra para o servidor Web, que por possuir endereço inválido, requer a realização de NAT (tradução de endereço) por parte do Firewall.
- Realização de login dos usuários remotos através de ID (identificação) e senha, sendo que além dos dados enviados pelo usuário, deve também ser armazenado a data e horário de conexão.
- Abrangência – BIOINFO.

4.3.3. Infra-estrutura

4.3.3.1. Segurança Física

Descrição

A infra-estrutura de informação deve estar bem protegida de qualquer tipo de ameaça física potencial, a fim de assegurar o desempenho de todos os componentes do sistema. A infra-estrutura vulnerável pode ser qualquer componente do sistema de computação, comunicação, rede, cabeamento, ou qualquer outro serviço de suporte ou utilidade necessário para manter funcionando o sistema de informação.

Muitos tipos de ameaça física são altamente direcionadas aos sistemas de informação. A infra-estrutura é atrativa porque é muito cara, freqüentemente é de fácil acesso e invasores nem sempre são pegos. Com freqüência, uma ataque físico é mais fácil de ser cometido e causa mais danos financeiros do que um ataque lógico.

A proteção física de um computador apresenta os mesmos problemas que são levantados quando se deseja proteger máquinas de escrever ou mesmo jóias. Como

uma máquina de escrever, um computador de escritório é um equipamento que muitas pessoas de dentro do escritório precisam acessar durante o trabalho. Como uma jóia, computadores são muito valiosos e fáceis de serem vendidos. Mas o perigo real em ter um computador roubado não diz respeito ao valor do hardware, mas ao valor da informação armazenada nestes. Da mesma forma que ocorre com registros oficiais ou financeiros, se não existe um backup, ou se o backup foi roubado junto com o computador, os dados roubados podem ficar irrecuperáveis. Mesmo tendo backup, deve-se gastar um bom tempo reconfigurando o sistema e restaurando os arquivos. Finalmente, existe sempre a chance da informação roubada, ou mesmo o fato desta ter sido roubada, ser usado contra os usuários do sistema.

Existem várias medidas a serem tomadas para proteger o sistema de computadores de ameaças físicas. Muitas destas medidas irão, simultaneamente, proteger o sistema de perigos naturais, de estranhos ou mesmo de sabotadores internos.

Uma segurança efetiva é um processo de planejamento, não um produto. Simplesmente escolhendo produtos, vendedores ou soluções padronizadas não é suficiente e podendo ser ineficiente, arriscado ou mesmo um desperdício. Sendo assim, o processo de planejamento é a chave para a boa proteção [9].

Motivação

A inexistência de identificação, principalmente por parte dos visitantes do laboratório, é um fator de risco, visto que a única forma de distinção entre as pessoas que freqüentam o laboratório é o conhecimento prévio dos usuários do local.

Em função da inexistência de identificação, outro fator de risco é a entrada não autorizada de estranhos, quando os próprios usuários do laboratório seguram a porta externa para que estes desconhecidos entrem no recinto.

Como os aparelhos de ar condicionado não possuem grades internas nem externas, basta a remoção dos mesmos para que se obtenha acesso à área restrita do laboratório, sem que seja necessário passar pelas portas de acesso.

Em situações emergenciais, não existe nenhum procedimento padrão que deve ser tomado para evacuar o local.

Medidas

- Instauração do uso de crachás, por parte dos visitantes ao laboratório.
- Instalação de um sistema de controle eletrônico de entrada e saída dos usuários, na porta de acesso ao laboratório.
- Instalação de grades de segurança na parte interna dos aparelhos de ar condicionado, impossibilitando o acesso direto à parte interior do laboratório quando da remoção destes.
- Criação de um procedimento de evacuação dos laboratórios (BIOMOL e BIOINFO) em casos emergenciais, a fim de que cada usuário possa executar uma determinada rotina padrão, em função da atividade que exerce. Sendo assim, os usuários dos laboratórios deverão estar cientes do procedimento de evacuação específico para a sua atividade de trabalho.
- Abrangência – BIOMOL e BIOINFO.

4.3.4. Metodologias

4.3.4.1. Recursos Humanos, gerenciamento e cuidados com a segurança dos empregados

Descrição

Segurança de Pessoal corresponde a tudo que envolve os usuários: A forma de contratá-los, seu treinamento, a monitoração de suas atividades e às vezes lidar com a demissão dos mesmos. Estatísticas mostram que a forma mais comum de ocorrência de crimes de invasão de computadores envolve as pessoas que têm acesso legítimo agora, ou que tiveram acesso recentemente. Alguns estudos mostram que cerca de

80% de incidentes são causados por estes indivíduos. Assim, o gerenciamento do pessoal com acesso restrito é uma parte importante de um plano de segurança [9].

As pessoas envolvem-se em problemas de segurança de computador de dois modos. Algumas pessoas, não intencionalmente ingressam na comissão de incidentes de segurança sem seguir um procedimento adequado, esquecendo de considerações de segurança, e não entendendo o que estão fazendo. Outras pessoas violam conscientemente controles e procedimentos para causar um incidente.

Motivação

Existe a necessidade de que todos os usuários dos laboratórios tenham conhecimento da forma de utilizar as instalações dos mesmos e expressem isto formalmente através da assinatura de documentação devida, para que riscos de segurança provenientes do desconhecimento das políticas vigentes sejam minimizados.

Medidas

- Inclusão de materiais escritos contendo as políticas de uso dos computadores e dependências por parte dos usuários, bem como as penalidades para violação destas políticas.
- Treinamento dos usuários para uso adequado das políticas de segurança.
- Todos os usuários devem assinar um termo de concordância com as políticas descritas acima e de suas restrições.
- Em caso de demissão de um usuário, fim de projeto ou trabalho, os responsáveis pela administração da rede devem ser imediatamente informados, para que sejam tomadas as medidas cabíveis à continuidade de acesso e a forma do mesmo por parte de tal usuário.
- Abrangência – BIOMOL e BIOINFO.

4.3.4.2. Classificação de informação

Descrição

Desde a antigüidade, as pessoas protegem as informações que lhes dão alguma vantagem sobre seus adversários. Em tempos de guerra, quando a soberania de uma nação está em jogo, as razões para se manter segredo sobre a informação são mais aparentes e aceitação dessas restrições pelas pessoas é mais abrangente.

Nos dias de hoje, seja nas empresas, nas universidades ou mesmo em órgãos governamentais, a necessidade de manter sigilo sobre determinado tipo de informação, enquanto outra modalidade deve se difundida, indica a necessidade de elaborar uma classificação de informação em vários níveis, cada um dos quais com seu nível de permissão de acesso.

Motivação

Informações de tipos diferentes precisam ser asseguradas de modos diferentes. Desta forma, um sistema de classificação é então requerido, onde a informação será classificada e os usuários terão acesso às informações em função das atividades desempenhadas, as quais determinarão quais tipos de dados os usuários podem acessar.

Medidas

Os dados devem ser classificados segundo o seguinte critério [5]:

Tipo 1 - Classificação: **Pública / Informação sem Classificação**

Os dados nestes sistemas podem se tornar públicos sem qualquer implicação para o laboratório, por exemplo os dados não são confidenciais. A integridade de dados não é vital. A perda destes dados devido a ataques maliciosos é um perigo aceitável.

Exemplos: Conteúdo informativo de interesse público.

Tipo 2 - Classificação: **Informação interna**

O acesso externo para estes dados será restrito, mas se estes dados tornarem-se públicos, as conseqüências não são críticas. O acesso Interno é seletivo e a Integridade de dados é importante mas não vital.

Exemplos: Arquivos do servidor (fora do banco de dados) e página Web do laboratório.

Tipo 3 - Classificação: **Informação confidencial**

Dados nesta classe são confidenciais dentro do laboratório e devem ser protegidos do acesso externo. Se estes dados forem acessados por pessoas sem autorização, poderiam influenciar todo o trabalho do laboratório, causar perda financeira importante, ou mesmo invalidar todo o resultado obtido. Integridade destes dados é vital.

Exemplo: Informações das seqüências biológicas contidas no banco de dados.

- Abrangência – BIOINFO.

4.3.4.3. Sistemas Críticos e controle de acesso a dados

Descrição

O acesso a dados e a informações está no centro de todo conjunto de Políticas de Segurança de Informação. Acesso indevido a dados pode infringir a política da organização e também os regulamentos legais.

Negar a pessoas sem autorização o acesso físico ou lógico aos sistemas da organização é parte de um processo de Segurança de Informação efetivo. Acesso físico à sala de computadores sempre deveria ser restrito somente a pessoas autorizadas.

Autorização [10] é a alocação da permissão à certos tipos de acessos à informações restritas. No mundo real, a autorização é conferida à seres humanos reais. Em contraste, a tecnologia da informação normalmente confere autorização à identificadores de usuários (IDs). Sistemas computacionais necessitam fazer a conexão entre IDs específicas e entre os usuários específicos destas IDs. Mesmo componentes inanimados, tais como placas de rede e impressoras precisam de um ID. *Identificação* [10] é o processo de associar um ID a um usuário ou a um computador ou componente de rede. *Autenticação* é o processo de conectar um ID a uma entidade específica. Por exemplo, a autenticação de uma identidade de usuário geralmente envolve a diminuição do número de possíveis entidades que desejam autorização de uso de uma ID específica para apenas uma pessoa.

Neste contexto, a segurança de sistemas críticos corresponde à necessidade de manter os dados de determinado sistema disponíveis e corretos.

Motivação

A **separação de obrigações** [10] é um modelo onde a cada indivíduo fica designada uma identificação (ID) e uma senha. Assim, programadores, administradores ou mesmo pesquisadores terão determinado nível de acesso, o qual é específico a cada atividade. Desta forma, existe a necessidade de que o acesso seja determinado pela necessidade, e não pelo *status*.

Sobre a determinação do acesso em função da necessidade, usuários cujas atividades não justificam o nível de acesso em que encontram, deveriam ser reclassificados e assim obter o nível de acesso adequado.

Além da necessidade de se fazer este controle de acesso aos dados, deve-se também realizar a proteção das informações contidas nos Bancos de Dados. Desta forma, ficará reduzida a possibilidade de modificação dos dados acidental ou intencional sem autorização.

Medidas

- Criação de grupos de usuários (remotos ou locais) com níveis de acesso específicos à atividade desempenhada. Cada usuário deve possuir uma identificação (ID) e uma senha intransferíveis.
- Cada usuário deve utilizar somente sua ID e senha para acessar o sistema.
- Abrangência – BIOINFO.

4.3.4.4. Proteção Antivírus

Descrição

O objetivo do conceito de proteção de vírus de computador é criar proteções satisfatórias com as quais a ocorrência de vírus de computador nos sistemas de tecnologia pode ser prevenida e detectada tão cedo quanto possível. Deste modo, medidas podem ser tomadas e possíveis danos podem ser minimizados. Na proteção contra vírus de computador é essencial que as proteções sejam adquiridas e as contramedidas técnicas sejam constantemente atualizadas. Esta exigência ocorre devido ao surgimento ininterrupto de novos vírus de computador ou variantes de vírus.

Embora exista a possibilidade do sistema de proteção, em determinado instante, não possuir ainda a capacidade de eliminar um vírus recém lançado, a sua implementação é indispensável atualmente.

Motivação

Existência descentralizada de um sistema de proteção antivírus (fica a critério de cada usuário utilizar ou não o antivírus) , bem como a ocorrência de infeções periódicas nos computadores.

Medidas

- Instalação de um sistema de proteção antivírus centralizado, onde a partir de um servidor é possível fazer o controle de instalações de software de antivírus em todas as estações;
- Configurar o sistema para que somente a partir do servidor seja possível a instalação de software antivírus;
- Fazer atualizações periódicas do software antivírus, e se possível programar para atualização automática;
- Promover verificações de rotina periódicas em todos os computadores do laboratório;
- Treinamento dos usuários para melhor uso do software antivírus e conscientização da necessidade do mesmo.
- Abrangência – BIOMOL e BIOINFO.

4.3.4.5. Procedimentos de Backup

Descrição

Backups são cópias de arquivos de dados ou registros. Normalmente, os backups são armazenados em uma mídia diferente do dado original.

Como resultado de uma falha técnica, deleção inadvertida ou manipulação não autorizada, os dados podem se tornar inúteis ou perdidos. A criação de backups, assim, assegura que qualquer dado redundante pode ser rapidamente restabelecido quando os dados operativos estão perdidos.

Backups devem ser um pré-requisito de qualquer operação segura em computadores, porém, a informação armazenada nas fitas é extremamente vulnerável. Quando a informação é armazenada em um computador, os mecanismos de verificação e proteção do sistema operacional previnem que pessoas não autorizadas vejam a informação. Depois que a informação é escrita em uma fita de backup, qualquer um que tiver posse da fita pode ler seu conteúdo. Por esta razão, a proteção dos backups se faz tão necessária quanto a proteção dos próprios computadores.

Motivação

Em função da freqüência da ocorrência de backup dos arquivos do sistema ser feita a critério do administrador, a inexistência de periodicidade programada para a realização do backup pode acarretar perdas de informação no caso de uma necessidade futura de restauração de arquivos do sistema.

Por não haver periodicidade nem etiquetação nas mídias de backup, a identificação dos arquivos onde foi feito backup em determinada data fica dificultada.

Como não existe modo de prevenção ao acesso à mídia de backup, qualquer pessoa que tiver acesso a estas mídias poderia restaurar os arquivos em outro sistema.

Medidas

- Estratégia de backup *Completo* uma vez na semana (por exemplo, Sexta-feira). Nesta estratégia é feito o armazenamento de uma cópia de todos os dados contidos no dispositivo de armazenamento do sistema (disco rígido).
- Estratégia de backup *Diferencial* nos demais dias da semana (Segunda a Quinta-feira, por exemplo). Nesta estratégia é feito o armazenamento de todos os dados que foram modificados desde o último backup *Completo*.
- Etiquetação das mídias de backup, as quais devem conter o dia da semana da realização do backup e o tipo de backup (Total ou Diferencial).
- Fazer uma verificação mensal dos backups para que se tenha certeza de que eles contém dados válidos.
- Utilizar encriptação nos dados de backup, a fim de dificultar o acesso à estes dados, em caso de extravio de mídia.
- Abrangência – BIOINFO.

4.3.4.6. Operações com computadores

Descrição

Operações consistem dos requerimentos para controle, manutenção e suporte dos sistemas de produção [10]. O pessoal responsável pela operação deve executar tarefas tais como instalar novas versões de programas em produção e manter a produção do banco de dados com eficiência máxima.

Motivação

A monitoração consistente da utilização dos recursos do sistema é uma das tarefas mais importantes do pessoal de operações. Através da monitoração é possível melhorar a eficiência da produção do banco de dados.

Freqüentemente, quando se faz necessário modificar uma pequena parte do Sistema Operacional, em vez de instalar uma nova versão, os fabricantes questionam se o usuário deseja aplicar uma atualização (*patch*). Os *patches* modificam localmente o código compilado.

Em função de muitos dos componentes do sistema ainda não possuírem número de patrimônio, faz-se necessária a diminuição do intervalo te tempo entre a aquisição de um componente e a colocação do patrimônio.

Medidas

- Ao proceder a instalação de um novo *patch*, primeiramente instalá-lo em uma máquina de testes, observar por um período se o sistema se comporta conforme esperado e só então executar a atualização nas outras máquinas que a requerem.
- Inclusão de análise gráfica e periódica dos arquivos de log para identificar mudanças no número de arquivos, disponibilidade de espaço em disco,

quantidade de CPU utilizada e número de operações de troca (*SWAP*) em memória virtual.

- Solicitação, assim que um novo componente de sistema for adquirido, da colocação de seu número de patrimônio.
- Abrangência – BIOINFO.

4.4. Conclusão

Neste capítulo foram descritas as 3 etapas de desenvolvimento dos procedimentos de segurança do Laboratório de Bioinformática. Por este laboratório estar inserido no Laboratório de Biologia Molecular (BIOMOL), alguns procedimentos se referiram também a este último.

Na primeira etapa (avaliação preliminar), os usuários do BIOINFO responderam ao questionário, que foi aplicado na forma de entrevista.

A segunda etapa foi realizada com o intuito de levantar um panorama da situação atual do BIOINFO. Os dados obtidos na etapa um, bem como uma descrição dos equipamentos existentes no mesmo, serviram de embasamento para realização desta tarefa.

Com os dados coletados e a análise das demandas de segurança existentes no BIOINFO e BIOMOL (quando se aplicava), foi realizada a etapa 3. Nesta fase foram descritos os Procedimentos de Segurança que já estavam em uso, os procedimentos de segurança que seriam implantados e aqueles tomados como sugestão futura de implantação. Para cada medida referente a um Procedimento de Segurança específico, foi determinada a abrangência desta (BIOMOL, BIOINFO ou ambos).

Capítulo 5 – Implantação

O capítulo 5 corresponde à Implantação do Firewall, bem como da configuração do HTTPS. A instalação do Firewall foi feita primeiramente em uma máquina de teste (uracila), sendo que após a verificação do seu perfeito funcionamento, procedeu-se a instalação no servidor definitivo, com a passagem dos arquivos necessários. Por motivo das duas instalações e procedimentos de configuração de arquivos serem equivalentes, são descritos nesta etapa apenas os passos referentes ao servidor definitivo (RNA).

5.1. Plano de implantação

A partir dos dados obtidos nas medidas de segurança aplicadas a cada subseção dos procedimentos de segurança (Capítulo 4), pode-se estabelecer um plano de prioridades para aplicação de tais medidas. A seqüência de implantação está descrita na tabela 5.1 :

PRIORIDADE	MEDIDA	APLICAÇÃO
	Sistemas Críticos e controle de acesso aos dados (4.3.4.3)	Já implantado
	Operações com computadores (4.3.4.6)	Já implantado
01	Instalação do Firewall (4.3.2.1)	Este projeto
02	Servidor Web e acesso remoto (4.3.2.3)	Este projeto
03	IDS – Sistema de Detecção de Intrusão (4.3.2.2)	Implantação futura
04	Procedimentos de Backup (4.3.4.5)	Implantação futura
05	Proteção Antivírus (4.3.4.4)	Implantação futura
06	Segurança Física (4.3.3.1)	Implantação futura
07	Classificação da Informação (4.3.4.2)	Implantação futura
08	Recursos Humanos, gerenciamento e cuidados com a segurança dos empregados (4.3.4.1)	Implantação futura

Tabela 5.1: Plano de Medidas do laboratório de Biologia Molecular

5.2. Instalação do OpenBSD

5.2.1. Visão geral do procedimento de instalação OpenBSD

O OpenBSD tem um procedimento de instalação muito robusto e adaptável. A maioria das arquiteturas têm um procedimento de instalação semelhante, o qual pode ser feito através de FTP, CDROM ou e arquivos de disco locais.

5.2.2. Arquiteturas de OpenBSD suportadas

O OpenBSD 3.1 suporta várias arquiteturas listadas abaixo em ordem alfabética:

```
alfa - DEC máquinas Alfa-baseadas.
amiga - Amiga modelos m68k-baseados
hp300 - Hewlett-Packard máquinas HP300/HP400.
i386 - PC's baseados na arquitetura Intel
mac68k - Maioria dos MC680x0-baseada modelos Apple Macintosh.
mvme68k - Motorola MVME147/16x/17x 68K cartões de VME.
macppc - Suporte para Apple baseada em sistemas de PowerPC.
sparc - Plataforma SPARC da Sun Microsystems
sparc64 - Sistemas de UltraSPARC da Sun
vax - Computadores VAX da Dec.
```

No caso da instalação no servidor do laboratório, a arquitetura utilizada foi a i386.

5.2.3. Criando CD de inicialização para o OpenBSD

Como o OpenBSD não fornece um ISO gratuito para instalação, foi adotada como opção a criação um CD bootável.

Para a criação deste CD, foram necessárias 3 etapas:

- Elaboração de um disquete de boot para instalação;
- Download dos arquivos de instalação;
- Gravação do CD.

5.2.3.1. Elaboração do disquete de boot

Para criação deste disquete, foi necessário o download de sua imagem de um dos sites do OpenBSD (http://www.openbsd.org/ftp.html). O arquivo de imagem utilizado foi o floppyB31.fs , proveniente de /pub/OpenBSD/3.1/i386/ .

Uma vez com a imagem, procedeu-se a instalação em um disquete, a qual foi feita através do rawrite, em ambiente Windows. Exemplo de uso:

```
C:\> rawrite
RaWrite 1.2 - Write disk file to raw floppy diskette

Enter source file name: floppyB31.fs
Enter destination drive: a
Please insert a formatted diskette into drive A: and press -ENTER- : >Enter<
```

5.2.3.2. Download dos arquivos de instalação

Assim como o download do arquivo de imagem, os arquivos de instalação também foram copiados de um dos sites descritos (http://www.openbsd.org/ftp.html), com caminho /pub/OpenBSD/3.1/i386/.

Os arquivos necessários para instalação são os seguintes:

- **base31.tgz** – Contém o sistema do OpenBSD **(Necessário).**
- **etc31.tgz** – Contém todos os arquivos do /etc **(Necessário).**
- **comp31.tz** – Contém o compilador e suas ferramentas, bibliotecas **(Recomendado).**
- **man31.tgz** – Contém as páginas do man **(Recomendado).**
- **misc31.tgz** - Contém informação de misc e documentação de setup.
- **game31.tgz** – Contém os jogos do OpenBSD.
- **xbase31.tgz** – Contém a instalação básica para X11.
- **xfont31.tgz** – Contém o servidor fonte X11.
- **xserv31.tgz** – Contém X server para X11.
- **xshare31.tgz** - Contém manpages, configurações locais, includes, etc para X.
- **bsd** – Este é o Kernel **(Necessário).**

5.2.3.3. Criação do CD de Boot

A instalação do CD de Boot foi feita através do programa Nero Burning ROM (http://www.ahead.de/en/index.html#c1002822566925), em ambiente Windows.

A opção de gravação utilizada foi CD-Rom Bootable, onde é possível selecionar o disquete de boot gravado para inicializar o CD. Então foram inseridos os arquivos e procedeu-se a gravação.

5.2.4. Inicializando as Imagens de Instalação do OpenBSD

Após gravado o CD, configurou-se a BIOS do computador para inicializar pelo CD. Assim, o computador foi ligado e a instalação inicializada, aparecendo a seguinte tela (Figura 5.1):

```
rootdev=0x1100 rrootdev=0x2f00 rawdev=0x2f02
 Enter pathname of shell or RETURN for sh:
 erase ^?, werase ^W, kill ^U, intr ^C
 (I)nstall, (U)pgrade or (S)hell? i
 ==================================================
 Welcome to the OpenBSD/i386 2.8 installation program.

 This program is designed to help you put OpenBSD on your disk in a simple and
rational way.

 As with anything which modifies your disk's contents, this program can cause
SIGNIFICANT data loss, and you are advised to make sure your data is backed up
before beginning the installation process.

 Default answers are displayed in brackets after the questions. You can hit
Control-C at any time to quit, but if you do so at a prompt, you may have to
hit return. Also, Quitting in the middle of installation may leave your system
in an inconsistent state. If you hit Control-C and restart the install, the
install program will remember many of your old answers.
You can run a shell command at any prompt via '!foo' or escape to a shell by
simply typing '!'.

Specify terminal type [pcvt25]: <Enter>
```

Figura 5.1: Tela inicial de instalação

Nas figuras referentes à instalação, as linhas mais escuras correspondem aos pontos de interação com o sistema. Os comandos executados estão em negrito ao final destas linhas. Algumas partes textuais onde não ocorreu interação com a console foram suprimidas das figuras, com o objetivo de facilitar a visualização dos procedimentos adotados.

5.2.5. Configurando os discos durante a instalação

A configuração do disco no OpenBSD é bastante semelhante para cada plataforma. Para a i386, a configuração do disco é feita em duas fases. Uma é com fdisk e a outra com disklabel. Foi selecionado o disco padrão sugerido com utilização de todo o espaço, conforme descrito a seguir:

```
The installation program needs to know which disk to consider the root disk.
Note the unit number may be different than the unit number you used in the
boot program (especially on a PC with multiple disk controllers).
Available disks are:

    sd0

Which disk is the root disk? [sd0] <Enter>
Do you want to use the *entire* disk for OpenBSD? [no] yes
[...]
```

Figura 5.2: Configuração de disco

5.2.6. Especificando os parâmetros de disco

Após a inicialização do disklabel (programa para formatação do disco e configuração das partições) pelo programa de instalação do OpenBSD, foi dado o comando p para exibir as informações dos parâmetros de disco existentes.

```
> p
device: /dev/rsd0c
type: ESDI
disk: ESDI/SCSI disk
label: Maxtor 54098U8
bytes/sector: 512
sectors/track: 63
tracks/cylinder: 16
sectors/cylinder: 1008
cylinders: 16383
total sectors: 80041248
free sectors: 80041185
rpm: 7200
16 partitions:
# size offset fstype [fsize bsize cpg]
a: 16450497 63 unused 0 0
c: 80041248 0 unused 0 0
```

Figura 5.3: Parâmetros de disco existentes.

Após a verificação dos parâmetros existentes, foi iniciada a configuração das partições. Os comandos iniciados por “a” são de criação e o iniciado por “d” são de deleção. A segunda letra se refere à partição criada.

O tamanho para cada partição variou em função da necessidade particular de espaço para cada um. A partição de *SWAP* teve como tamanho o dobro da memória física. No caso da partição */var* , o seu tamanho foi maior que o das outras partições porque nesta fica armazenado o arquivo de log.

A figura a seguir mostra como os parâmetros de disco foram especificados:

```
> d a
> a a
offset: [63] <Enter>
size: [4192902] 2g
Rounding to nearest cylinder: 164241 <Enter>
FS type: [4.2BSD] <Enter>
mount point: [none] /
> a b
offset: [4192965] <Enter>
size: [2104515] 1024m
Rounding to nearest cylinder: 614880 FS type: [swap] <Enter>
> a d
offset: [6297480] <Enter>
size: [4192964] 2g
Rounding to nearest cylinder: 164304 FS type:[4.2BSD] <Enter>
mount point: [none] /tmp
> a e
offset: [10490445] <Enter>
size: [41945715] 20g
Rounding to nearest cylinder: 164304 FS type: [4.2BSD] <Enter>
mount point: [none] /var
> a g
offset: [52436160] <Enter>
size: [10490445] 5g
Rounding to nearest cylinder: 716688 FS type: [4.2BSD] <Enter>
mount point: [none] /usr
> a h
offset: [62926605] <Enter>
size: [8193150] <Enter>
FS type: [4.2BSD] <Enter>
mount point: [none] /home
```

Figura 5.4: Criação das partições de disco.

Após a criação das partições, foi executado o comando p, a fim de exibir as configurações atuais de disco:

```
> p
device: /dev/rsd0c
type: ESDI
disk: ESDI/SCSI disk
label: Maxtor 54098U8
bytes/sector: 512
sectors/track: 63
tracks/cylinder: 16
sectors/cylinder: 1008
cylinders: 16383
total sectors: 80041248
free sectors: 0
rpm: 7200

16 partitions:
#        size    offset    fstype   [fsize bsize   cpg]
 a:   4192902        63    4.2BSD     1024  8192    16  # /
 b:   2104515   4192965      swap
 c:  71119692        63    unused        0     0
 d:   4192964   6297480    4.2BSD     1024  8192    16# /tmp
 e:  41945715  10490445    4.2BSD     1024  8192    16# /var
 g:  10490445  52436160    4.2BSD     1024  8192    16# /usr
 h:   8193150  62926605    4.2BSD     1024  8192    16# /home


> w
> q
```

Figura 5.5: Tabela de partições de disco

Para salvar esta configuração, executou-se o comando “w” (write) e posteriormente “q” (quit) para sair do disklabel.

5.2.7. Configurando o ponto de montagem e formatando o sistema de arquivos

Uma vez feita a distribuição das partições em disco, a configuração do ponto de montagem é feita apenas por confirmação dos parâmetros já existentes. Após esta fase, o instalador do OpenBSD inicializa o processo de formatação de arquivos. Estas etapas são descritas na figura abaixo:

```
The following partitions will be used for the root filesystem and swap:
        sd0a    /
        sd0b    swap

Mount point for sd0a (size=4192902k) [/, RET, none, or done]? >Enter<
Mount point for sd0e (size=41945715k) [/var, RET, none, or done]? >Enter<
Mount point for sd0g (size=10490445k) [/usr, RET, none, or done]? >Enter<
Mount point for sd0h (size=8193150k) [/home, RET, none, or done]? >Enter<
Mount point for sd0d (size=4192965k) [/tmp, RET, none, or done]? >Enter<
Mount point for sd0a (size=4192965k) [/, RET, none, or done]? done
Now you can select another disk to initialize. (Do not re-select a disk
you have already entered information for). Available disks are:

sd0

Which one? [done] >Enter<
You have configured the following devices and mount points:
sd0a /
sd0h /home
sd0d /tmp
sd0g /usr
sd0e /var
============================================================
The next step will overwrite any existing data on:
        wd0a wd0h wd0d wd0g wd0e

Are you really sure that you're ready to proceed? [n] y

Creating filesystems...
Warning: 63 sector(s) in last cylinder unallocated
/dev/rsd0a:     163422 sectors in 173 cylinders of 15 tracks, 63 sectors
        2GB in 11 cyl groups (16 c/g, 7.38MB/g, 1792 i/g)
Warning: 445 sector(s) in last cylinder unallocated
/dev/rsd0h:     7360160 sectors in 7789 cylinders of 15 tracks, 63 sectors
        4.3GB in 487 cyl groups (16 c/g, 7.38MB/g, 1792 i/g)
Warning: 1 sector(s) in last cylinder unallocated
/dev/rsd0d:     163484 sectors in 173 cylinders of 15 tracks, 63 sectors
        2GB in 11 cyl groups (16 c/g, 7.38MB/g, 1792 i/g)
/dev/rsd0g:     4193910 sectors in 4438 cylinders of 15 tracks, 63 sectors
        5GB in 278 cyl groups (16 c/g, 7.38MB/g, 1792 i/g)
Warning: 1 sector(s) in last cylinder unallocated
/dev/rsd0e:     163484 sectors in 173 cylinders of 15 tracks, 63 sectors
        20GB in 11 cyl groups (16 c/g, 7.38MB/g, 1792 i/g)
```

Figura 5.6: Configuração dos pontos de montagem e formatação.

5.2.8. Instalando a rede

A Configuração da rede é uma opção dentro do programa de instalação do OpenBSD. Neste ponto foram configuradas as interfaces de rede, a rota default e o servidor de nomes primário.

```
Configure the network? [y] >Enter<
Enter system hostname (short form, e.g. 'foo'): [] rna
If any interfaces will be configured using a DHCP server
it is recommended that you do not enter a DNS domain name,
a default route, or any name servers.
Enter DNS domain name (e.g. 'bar.com'): [] biomol.unb.br
You may configure the following network interfaces (the interfaces
marked with [X] have been successfully configured):

        [ ] fxp0
        [ ] bge0
        [ ] bge1
Configure which interface? (or 'done') [fxp0] >Enter<
IP address (or 'dhcp')? [] 164.41.88.201
Symbolic (host) name? [rna] >Enter<
Netmask? [255.255.255.0] >Enter<
Media directives? [] >Enter<
You may configure the following network interfaces (the interfaces
marked with [X] have been successfully configured):

        [X] fxp0
        [ ] bge0
        [ ] bge1
Configure which interface? (or 'done') [bge0] >Enter<
IP address (or 'dhcp')? [] 192.168.2.1
Symbolic (host) name? [rna] >Enter<
Netmask? [255.255.255.0] >Enter<
Media directives? [] >Enter<
You may configure the following network interfaces (the interfaces
marked with [X] have been successfully configured):

        [X] fxp0
        [X] bge0
        [ ] bge1
Configure which interface? (or 'done') [bge1] >Enter<
IP address (or 'dhcp')? [] 192.168.1.1
Symbolic (host) name? [rna] >Enter<
Netmask? [255.255.255.0] >Enter<
Media directives? [] >Enter<
You may configure the following network interfaces (the interfaces
marked with [X] have been successfully configured):

        [X] fxp0
        [X] bge0
        [X] bge1
Configure which interface? (or 'done') [done] >Enter<
Enter IP address of default route: [none] 164.41.88.1
Enter IP address of primary nameserver: [none] >Enter<
Would you like to use the nameserver now? [y] >Enter<
```

Figura 5.7: Configuração da rede

5.2.9. Escolhendo Mídia de Instalação e senha de root

Esta etapa descreve a escolha da senha de root e do tipo de instalação a ser usado, o qual será por CD. A figura 5.7 descreve o procedimento:

```
You will now be given the opportunity to escape to the command shell to do
any additional network configuration you may need. This may include adding
additional routes, if needed. In addition, you might take this opportunity
to redo the default route in the event that it failed above.
Escape to shell? [n] >Enter<
/dev/sd0a on /mnt type ffs (rw,asynchronous,local, ctime=Tue Jun 16 15:50:28 2
002)
/dev/sd0h on /mnt/home type ffs (rw,asynchronous,local, ctime=Tue Jun 16 15:50
:28 2002)
/dev/sd0d on /mnt/tmp type ffs (rw,asynchronous,local, ctime=Tue Jun 16 15:50:
28 2002)
/dev/sd0g on /mnt/usr type ffs (rw,asynchronous,local, ctime=Tue Jun 16 15:50:
28 2002)
/dev/sd0e on /mnt/var type ffs (rw,asynchronous,local, ctime=Tue Jun 16 15:50:
28 2002)
Please enter the initial password that the root account will have.
Password (will not echo): >enter root PW<
Password (again): >re-enter root PW<
Do you expect to run the X Window System? [y] >Enter<

You must now specify where the install sets you want to use are. They
must either be on a local device (disk, tape, or CD-ROM), na
accessible NFS filesystem or an accessible ftp or http network
server. You will have the chance to repeat this step or to extract
sets from several places, so you do not have to try to load all the
sets in one try and can recover from some errors.

Install from (f)tp, (h)ttp, (t)ape, (C)D-ROM or local (d)isk? c

Which CD-ROM contains the installation media? [cd0] >Enter<
Enter the directory relative to the mount point that contains the file:
[3.1/i386] >Enter<
```
Figura 5.8: Escolha da Mídia de Instalação e senha de root

5.2.10. Escolhendo os pacotes de instalação e finalizando

Nesta fase, foram selecionados todos os pacotes disponíveis para instalação, através da opção “*”. Uma vez escolhidos quais pacotes seriam instalados, foi questionado se realmente deseja-se proceder com esta. Uma barra de progresso foi mostrada, a qual manteve a informação sobre quanto tempo levaria a extração.

```
The following sets are available. Enter a filename, 'all' to select
all the sets, or 'done'. You may de-select a set by prepending a '-'
to its name.

        [X] base31.tgz
        [X] etc31.tgz
        [X] misc31.tgz
        [X] comp31.tgz
        [X] man31.tgz
        [X] game31.tgz
        [ ] xbase31.tgz
        [ ] xshare31.tgz
        [ ] xfont31.tgz
        [ ] xserv31.tgz
        [X] bsd
File name? [xbase31.tgz] *

        [X] base31.tgz
        [X] etc31.tgz
        [X] misc31.tgz
        [X] comp31.tgz
        [X] man31.tgz
        [X] game31.tgz
        [X] xbase31.tgz
        [X] xshare31.tgz
        [X] xfont31.tgz
        [X] xserv31.tgz
        [X] bsd
File name? [done] done

Ready to install sets? [y] >Enter<
Getting base31.tgz ...
100% |*********************************************| 23299 KB    00:25
Getting etc31.tgz ...
100% |*********************************************| 1164  KB    00:02
Getting misc31.tgz ...
100% |*********************************************| 1664  KB    00:01
Getting comp31.tgz ...
100% |*********************************************| 16061 KB    00:18
Getting man31.tgz ...
100% |*********************************************| 5412  KB    00:08
Getting bsd ...
100% |*********************************************| 4436  KB    00:02
Getting xbase31.tgz ...
100% |*********************************************| 8520  KB    00:06
Getting xshare31.tgz ... 100%
|**************************************************| 1815  KB    00:05
Getting xfont31.tgz ... 100%
|**************************************************| 30657 KB    00:31
Getting xserv31.tgz ... 100%
|**************************************************| 19339 KB    00:11
```

Figura 5.9: Escolha dos pacotes de instalação

5.2.11. Finalizando

Uma vez que os pacotes foram instalados, o passo final corresponde à configuração do fuso-horário, o qual foi realizado da seguinte maneira (Figura 5.9):

```
Extract more sets? [n]

Copying... fstab hostname.fxp0 hosts myname mygate resolv.conf ...done.

What timezone are you in? ('?' for list) [US/Pacific] /Brazil
Select a sub-timezone of 'Brazil' ('?' for list): East
You have selected timezone 'Brazil/East'.
Making all device nodes (by running /dev/MAKEDEV all) ...... done.
Installing boot block...
boot: /mnt/boot
proto: /usr/mdec/biosboot
device: /dev/rwd0c
/usr/mdec/biosboot: entry point 0
proto bootblock size 512
room for 12 filesystem blocks at 0x16f
Will load 7 blocks of size 8192 each.
Using disk geometry of 63 sectors and 255 heads.
 0: 56 @(0 152 8) (9583-9638)
 1: 40 @(0 153 1) (9639-9678)
 2: 16 @(0 9 27) (593-608)
/mnt/boot: 3 entries total
using MBR partition 3: type 166 (0xa6) offset 63 (0x3f)
Enabling machdep.allowaperture. Read xf86(4) for more information.
Cleaning up...
/dev/wd0e: unmount from /mnt/var
/dev/wd0g: unmount from /mnt/usr
/dev/wd0d: unmount from /mnt/tmp
/dev/wd0h: unmount from /mnt/home
/dev/wd0a: unmount from /mnt
Done.
CONGRATULATIONS!  You have successfully installed OpenBSD!  To boot the
installed system, enter halt at the command prompt. Once the system has
halted, reset the machine and boot from the disk.
# halt
syncing disks... done
The operating system has halted.
Please press any key to reboot.
```

Figura 5.10: Configuração de fuso-horário e finalização.

Desta forma, o OpenBSD foi instalado, seguindo então um boot para inicialização do sistema.

5.3. Configuração do HTTPS

O arquivo de configuração do servidor Web apache é o /etc/httpd/conf/httpd.conf. O arquivo httpd.conf é bem-comentado e até certo ponto auto-explicativo. Sua configuração padrão funciona para a maioria dos sites, assim não são necessárias muitas alterações neste arquivo.

Antes de iniciar a configuração do HTTPS no apache, foi feita uma cópia do arquivo existente, a qual foi nomeada como httpd.conf-old. Esta medida foi tomada como precaução, para que no caso da ocorrência de problemas, fosse possível restaurar a configuração padrão.

Para ter suporte ao HTTPS, o arquivo httpd.conf deve, primeiramente, estar configurado para também ouvir a porta 443 (porta padrão do SSL), como descrito neste trecho do arquivo:

```
##
##  SSL Support
##
##  When we also provide SSL we have to listen to the
##  standard HTTP port (see above) and to the HTTPS port
##
<IfDefine HAVE_SSL>
Listen 80
Listen 443
</IfDefine>
```

Para forçar clientes da Internet a usar a conexão HTTPS, foram inseridos os comandos:

```
RewriteEngine On
RewriteRule           /.*           https://www.biomol.unb.br/           [R]
```

5.4. Arquivo pf.conf

O pf (filtro de pacote ou packet filter) derruba, passa e modifica pacotes de acordo com as regras definidas neste arquivo. São usadas regras de filtragem para seletivamente passar o tráfego enquanto as regras de tradução especificam quais endereços serão mapeados e quais serão redirecionados. Para cada pacote inspecionado pelo filtro, o conjunto de regras é avaliado de cima para baixo, e a última regra coincidente decide que ação é executada. Regras devem estar em ordem: scrub, nat, filtro.

As regras de filtragem são avaliadas em ordem seqüencial, da primeira à última. Cada regra ou se encaixa ao pacote recebido ou não. A última regra que se encaixa ao pacote decide qual ação é tomada. Caso nenhuma regra se encaixe ao pacote, a ação padrão tomada é deixar o pacote passar (*pass*).

O funcionamento das regras é baseado na figura abaixo:
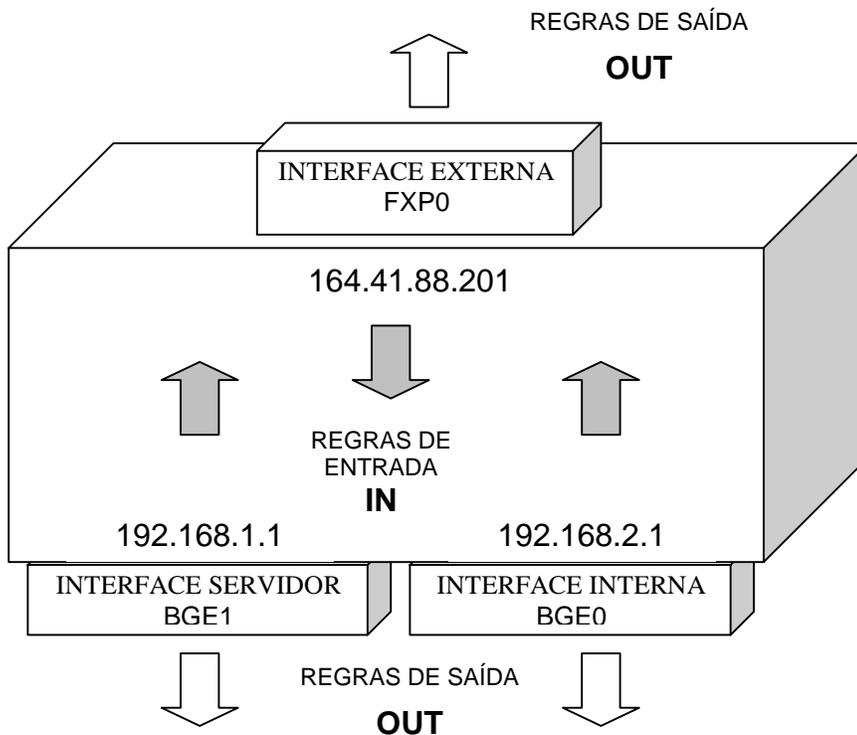
Figura 5.11: Funcionamento das regras do Packet Filter

Vamos tomar, por exemplo, uma regra da seguinte forma:

```
pass out log on $server_if proto udp from $int_net to $server_net keep state
```

Como esta regra é de “pass out“, ela refere-se à saída de pacotes, a qual está direcionada para a interface servidor (server_if). A origem dos pacotes é a rede interna (int_net) e o destino destes é a rede servidor (server_net). Assim, um pacote UPD, originário da rede interna, poderá acessar a rede servidor passando pela interface servidor.

A inicialização do arquivo pf .conf é feita pelo comando *pfctl*, da seguinte forma:

```
1. pfctl -F r
2. pfctl -F s
3. pfctl -R arquivo
```

O primeiro comando executa um descarregamento (flush) nas regras. O segundo comando executa um descarregamento da tabela de estados e o terceiro carrega o arquivo contendo as regras.

O arquivo pf.conf (em funcionamento) está definido com os seguintes parâmetros de configuração e regras, em ordem seqüencial:

5.4.1. Definições de macros

```
ext_if = "fxp0"
ext_if_addr = "164.41.88.201"
nat_addr = "164.41.88.202"
server_ext_addr = "164.41.88.203"
ext_net = "164.41.88.0/24"
ext_router = "164.41.88.1"
server_if = "bge1"
server_int_addr = "192.168.1.2"
server_net = "192.168.1.0/24"
int_if = "bge0"
int_net = "192.168.2.0/24"
invalid_nets = "10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 255.255.255.255/32"
```

As macros correspondem às seguintes definições:

Macro	Definição
ext_if	interface externa
ext_if_addr	endereço da interface externa
nat_addr	endereço de NAT
Server_ext_addr	endereço do servidor externo
ext_net	rede externa
ext_router	roteador externo
Server_if	interface servidor
Server_int_addr	endereço do servidor inerno
Server_net	rede do servidor
int_if	interface interna
int_net	rede interna
Invalid_nets	redes inválidas

Tabela 5.2: Definições das macros estabelecidas no arquivo pf.conf

5.4.2. Regra de Scrub

Considerando que algumas pilhas de IP não implementam corretamente a desfragmentação do pacote IP, o OpenBSD PF provê a diretiva de scrub. Se uma regra de scrub encontra o pacote, o componente de normalização PF garante que o mesmo está desfragmentado e completamente livre de todas as anormalidades, antes que seja enviado para seu destino final. Esta regra está declarada da seguinte forma:

```
# normalize all incoming traffic
scrub in log on $ext_if all
```

5.4.3. Regra de bloqueio de tudo por padrão

```
# block and log everything by default
block out log all
block in  log all
```

5.4.4. Regra para prevenir spoofing ou desconfiguração

Spoofing é a criação de pacotes de TCP/IP usando o endereço de IP de outra pessoa. Roteadores usam o endereço de IP de destino para remeter pacotes pela Internet, mas ignora o endereço IP de fonte. Aquele endereço só é usado pela máquina de destino quando ela responde à origem [12].

```
# block and log outgoing packets that don't have our address as source,
# they are either spoofed or something is misconfigured (NAT disabled,
# for instance), we want tobe nice and don't send out garbage.

block out log on $ext_if from ! $ext_if_addr to any
block out log on $ext_if from ! $nat_addr to any
block out log on $ext_if from ! $int_net to any
block out log quick on $ext_if from ! $server_net to any
```

Esta regra bloqueia a saída na interface externa, para qualquer endereço, de pacotes que não sejam originados: do endereço da interface externa ; do endereço de NAT ; da rede interna ou da rede do servidor.

5.4.5. Regra para derrubar pacotes de broadcast

```
# silently dropbroadcasts (cable modem noise)
block in log quick on $ext_if from any to 255.255.255.255
```

5.4.6. Regras da interface externa (conectada à rede externa)

5.4.6.1. Regras de ICMP

Este protocolo faz parte da Camada de Internet e usa o recurso de entrega do datagrama IP para enviar suas mensagens. ICMP envia mensagens que executam: Controle de Fluxo; Detecção de destinos inatingíveis; Redirecionamento de rota e Checagem de hosts remotos [13].

As regras de ICMP para a interface externa são as seguintes:

```
# pass out/in certain ICMP queries and keep state (ping)
# state matching is done on host addresses and ICMP id (not type/code),
```

```
# so replies (like 0/0 for 8/0) will match queries
# ICMP error messages (which always refer to a TCP/UDPpacket) are
# handledby the TCP/UDP states

pass out log on $ext_if inet proto icmp all icmp-type 8 code 0 keep state
pass in  log on $ext_if inet proto icmp all icmp-type 8 code 0 keep state
```

Esta regra permite a saída e entrada, na interface externa, de ICMP echo [14] (o que habilita o PING externo).

5.4.6.2. Regras de UDP

```
# pass out all UDP connections and keep state
pass out log on $ext_if proto udp all keep state

# pass in certain UDP connections and keep state (DNS)
pass in log on $ext_if proto udp from any to $ext_if_addr port = domain keep
state
```

A primeira regra de UDP habilita a saída de pacotes UDP para a rede externa. A segunda regra habilita a entrada de pacotes da rede externa direcionados à interface externa, caso a porta seja igual ao domínio.

O comando *keep state*, ao final das linhas corresponde a uma capacidade do pf de lembrar quais sessões TCP, UDP ou ICMP foram criadas, e filtrar os pacotes de acordo com com esta tabela de sessão. Quando o pf encontra um pacote cuja regra a ser aplicada possui o comando *keep state*, ele cria uma entrada na tabela de estados baseada na informação do pacote. Isto faz com que pacotes subseqüentes da mesma sessão possam passar pelo firewall sem que seja verificado no conjunto de regras.

5.4.6.3. Regras de TCP

```
# pass out all TCP connections and modulate state
pass out log on $ext_if proto tcp all modulate state

# pass in certain TCP connections and keep state (SSH, SMTP, DNS, IDENT)
pass in log on $ext_if proto tcp from any to $server_int_addr port { 22, http,
443 } keep state
pass in log on $ext_if proto tcp from any to $ext_if_addr port { 22, http, 443
} keep state
```

5.4.7. Regras da interface servidor

5.4.7.1. Regras UDP

As regras do protocolo UDP limitam a passagem (entrada e saída de certas conexões UDP).

```
# pass in and out certain UDP connections and keep state (DNS)
pass in log on $server_if proto udp from $server_net to any port = domain keep
state
pass in log on $server_if proto udp from $server_net to $int_net keep state
pass out log on $server_if proto udp from $int_net to $server_net keep state
```

A primeira regra libera a entrada de pacotes UDP na interface servidor, a partir da rede servidor, direcionados a qualquer porta igual ao domínio. A segunda e terceira regras liberam a passagem de pacotes UDP na interface servidor: oriundos da rede servidor para a rede interna (regra 2) e vice-versa (regra 3).

5.4.7.2. Regras TCP

```
# pass out all TCP connections and modulate state
pass in log on $server_if proto tcp from $server_int_addr to any port { 20,
21, 22, http, 443 } modulate state
pass out log on $server_if proto tcp from $int_net to $server_int_addr
modulate state
pass out log on $server_if proto tcp from any to $server_int_addr port { 22,
http, 443 } modulate state
```

As regras TCP para o servidor são descritas da seguinte forma:

- É liberada a entrada de pacotes TCP na interface servidor, oriundos do endereço da interface do servidor e destinados às portas 20, 21, http, 443 (SSL);
- É liberada a saída de pacotes TCP da interface servidor (no Firewall), oriundos da rede interna e destinados às portas 20, 21, 22, http e 443 (SSL) do servidor ;

- É liberada a saída de pacotes TCP da interface servidor, oriundos de qualquer endereço para o endereço da interno do servidor, desde que a porta de destino seja 22, http (80) ou 443 (SSL).

5.4.8. Regras da interface interna (conectada à rede interna)

5.4.8.1. Regras UDP

```
pass in log on $int_if proto udp from $int_net to any port = domain keep state
pass in log on $int_if proto udp from $int_net to $server_net keep state
pass out log on $int_if proto udp from $server_net to $int_net keep state
```

A primeira regra permite a entrada de pacotes na interface interna (para dentro do Firewall), oriundos da rede interna para qualquer porta igual a domínio. A segunda regra permite a entrada de pacotes na interface interna, provindos da rede interna para a rede do servidor. A terceira regra permite a saída de pacotes da interface interna, oriundos da rede do servidor para a rede interna.

5.4.8.2. Regras TCP

```
pass in log on $int_if proto tcp from $int_net to any keep state
pass in log on $int_if proto tcp from $int_net to $server_net keep state
```

As regras de TCP para a rede interna permitem:

- Entrada na interface interna de pacotes do protocolo TCP, oriundos da rede interna e com qualquer destino;
- Entrada na interface interna de pacotes do protocolo TCP, oriundos da rede interna para a rede servidor.

5.5. Arquivo resolv.conf

O arquivo *resolv.conf* especifica como a rotina *resolver* (usada para fazer, enviar e interpretar solicitações ao Servidor de Domínio da Internet) deve operar. O *resolv.conf* contém a informação que é lida pela rotina do *resolver.* Este arquivo é editável e contém uma lista de palavras-chave com valores que fornecem vários tipos de informação ao *resolver.*

Segue o arquivo *resolv.conf* existente em */etc.*

```
search biomol.unb.br
nameserver 127.0.0.1
;nameserver 164.41.88.201
lookup file bind
```

Na primeira linha, o comando *search* é utilizado para explicitar o servidor de domínio local.

A segunda linha inicia com o comando *nameserver*, o qual indica o endereço ipv4 do servidor de domínio utilizado pelo resolver para realizar buscas (*queries*). Geralmente (e neste caso), o *nameserver* utilizado é o da máquina local.

A Quarta linha refere-se ao comando *lookup*, o qual é utilizado pelas rotinas *gethostbyname* e *gethostbyaddr* para especificar quais bases de dados serão pesquisadas, no intuito de resolver o host por nome ou endereço. As opções indicadas no arquivo são *bind* (utiliza o DNS para efetuar a busca) e *file* (busca por entradas em */etc/hosts*).

5.6. Arquivos rc.conf e rc.local

O arquivo rc.conf contém uma séries de designações de sintaxe usadas para configurar o *daemon* do sistema. Apesar de não ser lido pelo *kernel*, ele é utilizado pelo arquivo *rc*, o qual possui scripts de comando para inicialização de sistema. A designação de sintaxe a ser destacada neste arquivo é aquela que habilita o *packet filter,* conforme descrito abaixo:

```
pf=YES                  # Packet filter / NAT
```

O arquivo *rc.local* é executado ao fim do *rc*, e possui comandos e *daemons* que não são parte da instalação original. A parte deste arquivo referente aos comandos adicionais é a seguinte:

```
# Log do firewall em arquivo texto
echo "Starting Firewall log"
/usr/sbin/tcpdump -n -e -ttt -l -s 1500 -i pflog0 > /var/log/fw.log &

# alias for ext_if (xl0)
# nat_addr
ifconfig fxp0 alias 164.41.88.202 netmask 255.255.255.0
# server_addr
ifconfig fxp0 alias 164.41.88.203 netmask 255.255.255.0
```

O primeiro comando realiza o armazenamento do arquivo *pflog0* em */var/log/fw.log*. Os parâmetros são assim definidos:

- -n Não faz a conversão de endereços para nomes.
- -e Imprime o nível de link do cabeçalho em cada linha de dump.
- -ttt Imprime o dia e mês no timestamp.
- -l Buferiza a linha de saída (para ver os dados enquanto são capturados).
- -s Analisa os primeiros 1500 bytes de dados de cada pacote (igual à mtu).
- -i Ouve as inferfaces.

Os comandos seguintes criam um alias para a interface externa fxp0, referentes ao endereço de NAT (164.41.88.202) e ao endereço do servidor Web (164.41.88.203).

5.7. Arquivo nat.conf

Este é o arquivo “nat.conf” que está rodando na máquina “RNA” do Laboratório de Biologia Molecular:

```
#      $OpenBSD: nat.conf,v 1.4 2001/07/09 23:20:46 millert Exp $
#
# See nat.conf(5) for syntax and examples
#
# replace ext0 with external interface name, 10.0.0.0/8 with internal network
# and 192.168.1.1 with external address
#
# nat: packets going out through ext0 with source address 10.0.0.0/8 will get
# translated as coming from 192.168.1.1. a state is created for such packets,
# and incoming packets will be redirected to the internal address.

# nat on ext0 from 10.0.0.0/8 to any -> 192.168.1.1

# rdr: packets coming in through ext0 with destination 192.168.1.1:1234 will
# be redirected to 10.1.1.1:5678. a state is created for such packets, and
# outgoing packets will be translated as coming from the external address.

# rdr on ext0 proto tcp from any to 192.168.1.1/32 port 1234 -> 10.1.1.1 port 567

# DNA
nat on fxp0 from 192.168.2.0/24 to any -> 164.41.88.202

# estacoes de trabalho
binat on fxp0 from 192.168.1.1 to any -> 164.41.88.203
#binat on fxp0 from 192.168.1.1 to ! 192.168.2.0/24 -> 164.41.88.203
```

A regra explicita o NAT na interface externa (fxp0) originário de qualquer endereço da rede servidor para a rede externa, direcionados para o endereço 164.41.88.202 (endereço de NAT).

A segunda regra prevê um NAT bidirecional na interface externa (fxp0) originário da interface da rede interna (bge1) para o endereço 164.41.88.203

5.8. Arquivo sysctl.conf

```
#     $OpenBSD: sysctl.conf,v 1.25 2002/02/23 08:07:58 deraadt Exp $
#
# This file contains a list of sysctl options the user wants set at
# boot time.  See sysctl(3) and sysctl(8) for more information on
# the many available variables.
#
net.inet.ip.forwarding=1      # 1=Permit forwarding (routing) of packets
net.inet.tcp.recvspace=65535  # Aumentar performance de transferencia dado
net.inet.tcp.sendspace=65535  # Idem
#net.inet6.ip6.forwarding=1   # 1=Permit forwarding (routing) of packets
#net.inet6.ip6.accept_rtadv=1 # 1=Permit IPv6 autoconf (forwarding must be 0)
#net.inet.tcp.rfc1323=0       # 0=disable TCP RFC1323 extensions (for if tcp
#is slow)
#net.inet.esp.enable=0        # 0=Disable the ESP IPsec protocol
#net.inet.ah.enable=0         # 0=Disable the AH IPsec protocol
#net.inet.ipcomp.enable=1     # 1=Enable the IPCOMP protocol
#ddb.panic=0                  # 0=Do not drop into ddb on a kernel panic
#ddb.console=1                # 1=Permit entry of ddb from the console
#fs.posix.setuid=0            # 0=Traditional BSD chown() semantics
#vm.swapencrypt.enable=1      # 1=Encrypt pages that go to swap
#vfs.nfs.iothreads=4          # number of nfsio kernel threads
#net.inet.ip.mtudisc=0        # 0=disable tcp mtu discovery
#kern.usercrypto=1            # 1=enable userland use of /dev/crypto
#machdep.allowaperture=2      # See xf86(4)
#machdep.apmwarn=10           # battery % when apm status messages enabled
#machdep.apmhalt=0            # 1=powerdown hack, try if halt -p doesn't work
#machdep.kbdreset=1           # permit console CTRL-ALT-DEL to do a nice halt
```

O arquivo sysctl.conf contém uma lista de opções para controle do sistema. Estas opções são carregadas no momento da inicialização. As opções habilitadas são `net.inet.tcp.recvspace=65535` e `net.inet.tcp.sendspace=65535` que prevêem um aumento na performance de transferência, tanto no envio quanto no recebimento. O parâmetro `net.inet.ip.forwarding=1` que também está habilitado, está explicitado na seção 5.14.2.

5.9. Arquivo syslog.conf

```
#	$OpenBSD: syslog.conf,v 1.12 2001/08/23 13:27:52 camield Exp $
#
*.err;kern.debug;auth.notice;authpriv.none;mail.crit       /dev/console
*.notice;auth,authpriv,cron,ftp,kern,lpr,mail,user.none    /var/log/messages
kern.debug,user.info,syslog.info                           /var/log/messages
auth.info                                                  /var/log/authlog
authpriv.debug                                             /var/log/secure
cron.info                                                  /var/cron/log
daemon.info                                                /var/log/daemon
ftp.info                                                   /var/log/xferlog
lpr.debug                                                  /var/log/lpd-errs
mail.info                                                  /var/log/maillog
#uucp.info                                                 /var/log/uucp
*.err                                                      root
*.notice;auth.debug                                        root
*.alert                                                    root
*.emerg                                                    *

#*.notice;auth,authpriv,cron,ftp,kern,lpr,mail,user.none   @loghost
#kern.debug,user.info,syslog.info                          @loghost
#auth.info,authpriv.debug,daemon.info                      @loghost

#!sudo
#*.*                                                       /var/log/sudo
#!chat
#*.*                                                       /var/log/chat
# Firewall
#local1.*                                            /var/log/fwsyslog.log
local1.*                                             @loghost
```

O arquivo syslog.conf é o arquivo de configuração para o programa syslogd. Consiste em blocos de linhas separados por especificações de programa com cada linha contendo dois campos: o campo seletor, que especifica os tipos de mensagens e prioridades para as quais a linha aplica, e um campo de ação que especifica a ação a ser tomada se uma mensagem que o syslogd combina com os critérios de seleção.

5.10. Arquivos de Interfaces de Rede

Neste projeto utilizou-se, na máquina RNA, três interfaces de rede. Uma para conexão com a rede externa (fxp0), a segunda para conexão com o servidor (bge1) e a terceira utilizada conexão com a rede interna, conforme descrito no procedimento de instalação (5.2.8). Abaixo, serão descritos os arquivos relativos ao funcionamento destas interfaces:

- hostname.fxp0

```
inet 164.41.88.201 255.255.255.0 NONE
```

- hostname.bge0

```
inet 192.168.2.1 255.255.255.0 NONE
```

- hostname.bge1

```
inet 192.168.1.1 255.255.255.0 NONE
```

Nestes arquivos observa-se, primeiramente, o endereço IP da interface e logo em seguida o endereço IP da máscara de rede.

5.11. Arquivo mygate

```
164.41.88.1
```

Arquivo onde se encontra o gateway padrão.

5.12. Arquivo myname

```
rna
```

Arquivo onde se encontra o nome da máquina, configurado durante o processo de instalação.

5.13. Arquivo Hosts

O arquivo hosts contém informações relativas aos hosts conhecidos na rede. Para cada host uma única linha deve ser apresentada com a seguinte informação:

```
endereço_internet             hostname_oficial             alias
```

Para o este caso, tem-se

```
127.0.0.1         localhost.biomol.unb.br       localhost
164.41.88.201     rna.biomol.unb.br             rna
164.41.88.202     uracila.biomol.unb.br         uracila
```

5.14. Outros procedimentos de configuração

5.14.1. Identificando e Configurando as Interfaces de Rede

No OpenBSD, são nomeadas interfaces pelo tipo da placa, e não pelo tipo de conexão. Pode-se ver que a placa de rede é inicializada durante o processo de Boot ou usando o comando *dmesg*, depois do processo de Boot. Também tem-se a chance de visualizar a interface de rede usando o comando *ifconfig*. Por exemplo, este é resultado do comando *dmesg* para uma placa de rede *ne2k* que usa o *ne* como nome de dispositivo.

```
ne3 at pcmcia1 function 0 "Linksys, EtherFast 10/100 PC Card (PCMPC100), "
port 0x340/16 irq 9
ne3: address 00:e0:98:04:95:ba
```

Novamente pode-se verificar quais as interfaces foram identificadas utilizando o comando *ifconfig*. Esta é a saída do comando para um dispositivo *ne2k.*

```
$ ifconfig -a
    lo0: flags=8009<UP,LOOPBACK,MULTICAST>
            inet 127.0.0.1 netmask 0xff000000
    lo1: flags=8008<LOOPBACK,MULTICAST>
    ne3: flags=8863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST>
            media: Ethernet manual
            inet 10.0.0.38 netmask 0xffffff00 broadcast 10.0.0.255
    sl0: flags=c010<POINTOPOINT,LINK2,MULTICAST>
    sl1: flags=c010<POINTOPOINT,LINK2,MULTICAST>
    ppp0: flags=8010<POINTOPOINT,MULTICAST>
    ppp1: flags=8010<POINTOPOINT,MULTICAST>
    tun0: flags=10<POINTOPOINT>
    tun1: flags=10<POINTOPOINT>
    enc0: flags=0<>
    bridge0: flags=0<>
    bridge1: flags=0<>
```

5.14.2. Configurando o OpenBSD como um Gateway

Esta é a informação básica que se precisa para montar o OpenBSD como um gateway (também chamado de roteador).

O kernel padrão já tem a habilidade para permitir IP Forwarding, mas foi necessário uma recompilação. Para mudar isto permanentemente editou-se o arquivo /etc/sysctl.conf a fim de permitir o IP Forwarding. Foi adicionada esta linha naquele arquivo de configuração.

```
net.inet.ip.forwarding=1
```

Para fazer esta mudança sem reiniciar foi usado o utilitário sysctl diretamente. Entretanto esta mudança já não existirá depois de uma reinicialização, e precisa ser rodado como root.

```
# sysctl -w net.inet.ip.forwarding=1
net.inet.ip.forwarding: 0 -> 1
```

5.15. Conclusão

Neste capítulo foram descritos todos os passos percorridos, desde a instalação até a configuração dos arquivos que controlam a maneira com a qual o firewall se comportará. Pode-se citar com mais ênfase a parte onde são feitos os acertos para o funcionamento do HTTPS e do arquivo pf.conf. É válido lembrar que além disso foram configurados os arquivos nat.conf e sysctl.conf bem como os arquivos relacionados às interfaces de rede, a fim de completar sua implementação.

Capítulo 6 – Dificuldades e sugestões futuras

6.1. Problemas encontrados

Durante o Desenvolvimento dos procedimentos de segurança, a maior dificuldade encontrada foi a inexistência de um modelo que pudesse atender completamente as necessidades existentes no Laboratório. Assim, foram utilizados como base dois modelos de políticas de segurança existentes, o *RFC2196* [3] (Site Security Handbook) e o *IT Baseline Protection Manual* [4].

Na parte de implementação, uma dificuldade encontrada foi a de fazer a leitura do log de dados coletados em formato de texto. Apesar deste problema, os dados estão sendo coletados e armazenados em formato binário.

6.2. Trabalhos Futuros

Como visto no capítulo 5, seria de grande importância a continuidade do Plano de Implantação de Medidas de Segurança, dentre as quais podem ser citadas:

- IDS - Sistema de Detecção de Intrusão (4.3.2.2);
- Procedimentos de Backup (4.3.4.5);
- Proteção Antivírus (4.3.4.4);
- Segurança Física (4.3.3.1);
- Classificação da Informação (4.3.4.2);
- Recursos Humanos, gerenciamento e cuidados com a segurança dos empregados (4.3.4.1).

Um Sistema de Detecção de Intrusão, colocado na rede interna do laboratório (dentro do Firewall) poderia auxiliar este, na medida em que o log deste auxiliaria na determinação do nível de funcionalidade do Firewall. O IDS poderia também ser colocado na rede externa, o qual auxiliaria a identificar o nível de ameaça a que uma rede está sujeita.

A implantação de procedimentos periódicos de backup auxiliariam na garantia da restauração dos dados, caso algum problema ocorresse com os dados em disco. Backups *Completos* uma vez na semana e *Diferenciais* nos outros dias (exceto Sábado e Domingo) fariam parte dos procedimentos, assim como etiquetação das fitas e encriptação dos dados contidos nestas.

A Instalação de um sistema de proteção antivírus centralizado, com controle de atualização das estações seria outra parte do plano de implantação futuro. Este procedimento possui um diferencial em relação aos anteriores, pois até o momento só existem soluções proprietárias com alto grau de confiabilidade. Sua implantação dependeria de um orçamento próprio, o qual serviria para sua compra e manutenção.

Sobre os procedimentos em Segurança Física, medidas como instalação de um sistema de controle eletrônico na entrada e saída e instalação de grades no ar condicionado também dependem de orçamento para sua viabilização. No caso da instauração do uso de crachás, existe também a necessidade de haver um funcionário fazendo o controle da distribuição e recolhimento destes, bem como a anotação dos dados dos visitantes.

Um sistema de classificação de informação também facilitaria a distribuição das permissões de usuário, pois diria o nível de confidencialidade da informação que determinada pessoa precisa acessar.

Para trabalhos futuros, fica também como sugestão a inclusão de materiais escritos contendo as políticas de segurança do laboratório, bem como o treinamento dos usuários para uso adequado destas políticas.

6.3. Conclusão

Este capítulo cita alguns complementos que podem ser incorporados com o intuito de melhorar a segurança e a consistência do sistema, evitando possíveis perdas ou danos os quais o firewall, sozinho, não tem condições de prevenir ou reparar.

Capítulo 7 – Conclusão

Sobre os objetivos descritos para este projeto, no Capítulo 1, pode-se dizer que eles foram atingidos. Tanto a implementação do Firewall quanto o Desenvolvimento dos Procedimentos de Segurança foram bem sucedidos.

Após diversas etapas como levantamento de dados, pesquisa, aplicação de questionários e implantação do Firewall, percebeu-se a importância das contribuições trazidas pelo trabalho realizado.

O Desenvolvimento dos Procedimentos de Segurança do Laboratório trouxeram um alicerce para esta difícil tarefa que é identificar as vulnerabilidades existentes no local. Com a descrição dos motivos pelos quais estas vulnerabilidades foram levantadas e a especificação das medidas necessárias para minimizá-las, os Procedimentos de Segurança constituíram o ponto de partida para a implantação das Medidas de Segurança necessárias.

A fase de aplicação de questionário foi de enorme contribuição, principalmente pela interação com os usuários do laboratório, onde estes puderam explicitar suas sugestões de medidas de segurança.

Na fase de Desenvolvimento dos Procedimentos foi possível ter uma idéia do quanto de informação sobre os mais diversos tópicos de segurança existem, seja em livros, publicações científicas ou mesmo em sites de órgãos governamentais.

Na implantação do Firewall, pode-se ter uma idéia de que segurança não diz respeito somente a instalação de determinado hardware com o objetivo de controlar o tráfego em uma rede. Esta engloba também poder estabelecer um equilíbrio entre as necessidades do grupo e a minimização dos riscos de segurança conseqüentes desta necessidade. Além disso, nenhuma caixa fechada que seja vendida pode atender de pronto a uma demanda específica de um local. Além da eficiência, a adequação com as necessidades faz do Firewall um equipamento tão específico para uma rede quanto os serviços que precisam rodar nesta.

Ressalta-se que este trabalho não tem por objetivo ser um documento definitivo. Necessidades futuras, neste mesmo laboratório, podem demandar outros Procedimentos de Segurança, ou mesmo reestruturação dos antigos. No caso do

Firewall, novos alertas de possíveis vulnerabilidades, novas formas de ataques ou mesmo outros serviços, que porventura sejam inseridos no sistema, demandam um cuidado freqüente com o mesmo.

Espera-se que este trabalho seja continuado e que sua contribuição seja válida para outros projetos nesta mesma área. Em seu desenvolvimento, este projeto trouxe um modelo prático de Procedimentos de Segurança, o qual poderá ser tomado como ponto de partida para o desenvolvimento de novos projetos de segurança em outros laboratórios com necessidades afins.

Como dito no início deste trabalho, apenas com um estudo detalhado dos problemas potenciais e implantação das alterações sugeridas, uma rede e seus componentes poderão atender às expectativas voltadas a eles. Apesar de não existir um modelo de segurança perfeito, a implementação de Procedimentos de Segurança pode minimizar o efeito de problemas desta natureza.

Anexo 1 – Questionário de Avaliação Preliminar

1.1. Estado da política atual

As questões seguintes não só coletam informações de base sobre a política de segurança, como também determinam se os usuários (empregados) possuem alguma idéia sobre quem é responsável pela determinação de tal política.

- O laboratório possui alguma política de segurança ?
- Quem a desenvolveu ? Um indivíduo ? Um grupo ?
- Aonde e como(papel, eletrônico) a política de segurança está disponível ?
- Quando as políticas foram atualizadas pela última vez ?
- Quem, se alguém, tem a responsabilidade explícita de manter as políticas ?
- Quem implementa a política de segurança a nível do laboratório ?
- A quem o responsável pela segurança é subordinado ?
- Quem monitora a concordância com as políticas de segurança e padrões ?

1.2. Classificação de Dados

- Existem níveis de classificação da segurança aplicáveis ao seu trabalho ? Se sim, como eles são chamados ?

- Existem regras que determinam se a informação que você trabalha deve ser classificada com um nível particular de confidencialidade ?

- Existem documentos ou arquivos rotulados para mostrar seu nível de segurança ?

- Qual é sua opinião sobre o valor de tal classificação ?

- As pessoas em seu grupo prestam atenção às classificações do nível de segurança ?

- Você possui alguma sugestão para melhoria da classificação dos dados ?

1.3. Sistemas Sensíveis

As questões nesta seção focam a informação que deve ser controlada contra revelação não autorizada e disseminação;

- Em seu trabalho, existe algum tipo de informação, documentos ou sistemas que você acredita que deveriam estar protegidos contra revelação não autorizada ?

- Como você pessoalmente protege a informação sensível que você lida ?

- De maneira anônima, como as outras pessoas do laboratório lidam com as informações sensíveis ?

- Que você saiba, houve algum problema com a revelação de informação sensível no laboratório ?

- Você tem alguma sugestão para melhorar o modo como se lida com a informação sensível ?

1.4. Sistemas Críticos

As questões nesta seção focam a informação que necessita de atenção especial quanto à disponibilidade e exatidão.

- Em seu trabalho, existe algum tipo de informação, documentos, ou sistemas que você sente serem críticos a ponto de serem protegidos contra modificação não autorizada ou destruição ? Caso positivo, nomeie-os.

- Existe alguma precaução especial usada por você quanto à guarda de informação crítica em sua área ?

1.5. Autenticidade

- Você sabe de algum caso onde alguém tenha usado de outra identidade para enviar e-mails, faxes ou cartas ? Caso positivo, houveram conseqüências ?

- Alguém no seu grupo usa assinatura digital ou documentos eletrônicos ?

- Alguém no seu grupo usa ou faz cópias de algum sistema proprietário ? Caso positivo, você acha que existe algum problema nisso ?

1.6. Exposição

- Quais são as piores conseqüências que você pode imaginar que resultariam da publicação (divulgação) da informação mais sensível que você possui ?

- O que aconteceria, na sua opinião, se concorrentes obtivessem a informação confidencial específica que você controla em sua área ?

- Você pode estimar custos monetários associados com a questão descrita acima ?

- Quais seriam as piores conseqüências que você poderia prever se a informação crítica com a qual você trabalha fosse alterada sem autorização ou por meio acidental ?

- O que aconteceria se você não pudesse acessar a informação crítica de maneira rápida o suficiente para realizar seu trabalho ?

- Você pode imaginar os custos destas brechas de disponibilidade de dados e integridade de dados ?

- Haveria problema se alguém forjasse documentos em seu nome ou em nome do laboratório ? Você poderia esboçar algum cenário e mostrar os custos resultantes destas brechas de autenticidade ?

1.7. Recursos humanos, gerenciamento e cuidados com a segurança do pessoal

- Do seu conhecimento, quem é o responsável pelo desenvolvimento das políticas de segurança ?

- Você sabe onde encontrar as políticas de segurança que se aplicam ao seu trabalho ?

- Quando, se alguma vez, você se lembra de ter assinado algum documento concordando com as políticas de segurança ?

- Quem é responsável pela monitoração da concordância com as políticas de segurança no laboratório ? E no departamento ?

- Você já recebeu algum treinamento em políticas de segurança ? Caso positivo, quando foi a última vez ?

- Você já viu algum material escrito circulando em seu grupo de trabalho que discuta segurança de informação ?

- Você acredita que proteger a informação do laboratório é uma de suas responsabilidades oficiais ?

1.8. Segurança Física

- Alguém confere a sua identificação quando você entra no departamento (subsolo) ?

- Existe algum sistema eletrônico de controle de acesso limitando o acesso a sua área de trabalho ? o que é ?

- As pessoas seguram a porta para que outros estranhos entrem em área segura ? Você faz o mesmo ?

- As pessoas deixam a área em que trabalham (laboratório) aberto em períodos onde ninguém se encontra no recinto ?

- As pessoas que trabalham no laboratório usam crachás de identificação ?

- Os visitantes usam crachás ?

- Você já viu visitantes em sua área de trabalho sem estar usando crachás ?
- O que você faria se você visse um estranho sem identificação na área que você trabalha ?
- Você tranca alguma parte da sua mesa de trabalho quando você sai do recinto do laboratório ?
- O que você faria se ouvisse um alarme de incêndio ?
- Aonde é o extintor de incêndio mais próximo ?
- O que você faria se alguém precisasse de atenção médica ?
- Existe algum posto de tratamento médico nas proximidades ?
- Existe alguém qualificado para fazer massagem cardio-pulmonar no recinto ? Caso positivo, esta possui identificação ?
- Você teve algum treinamento sobre o que fazer em caso de emergência ? Você foi treinado para evacuar a área ?
- Existe alguma coisa que você acredita que possa ser melhorada sobre a segurança física ?

1.9. Segurança das operações com computadores

- Quanto você aguarda, após o lançamento de novas versões do sistema operacional em uso, para atualizar as máquinas em produção ?
- Como você coloca o novo software em produção ?

- Como você lida com relatos de problemas ? Você possui algum sistema automatizado de recepção de problemas ?

- Pessoas de fora do laboratório podem acessar as máquinas deste ?

- Pessoas contratadas, incluindo técnicos de reparo, podem circular pela área restrita sem estar acompanhados ?

- O pessoal da limpeza circula pela área restrita sem que haja alguém do grupo do laboratório presente ?

- Os componentes do sistema possuem número de identificação de patrimônio ?

- Existe um sistema de permanência de alimentação de energia, em caso de queda da energia externa ? Isto inclui o ar condicionado ?

- Existem registros para os momentos onde o sistema ficou fora do ar ? Quantas vezes isto ocorreu nos últimos 3 meses ? E no último ano ?

- Quem monitora a utilização de recursos do sistema ? Existem relatórios otimizados mostrando a utilização de disco, CPU ou largura de banda ?

- Quais melhorias em segurança das operações de computadores você gostaria de ver implementadas ?

1.10. Controle de acesso a dados

- Você precisa de identificação para acessar o computador e a rede com a qual você trabalha ?

- Você possui um (ID) que não é compartilhado com ninguém ?

- Você precisa de utilizar uma senha para iniciar o uso do seu computador ?

- Você já compartilhou a sua senha com alguém ? Você já pegou a senha de alguém emprestado ? Caso positivo, conte em que situação isto ocorreu.

- Existem limitações quanto à permissão de uso da informação que você trabalha ?

- Existe informação que você possa ver mas não possa alterar ?

- Você usa encriptação com alguma informação de trabalho ?

- Existem laptops para uso pessoal ? A informação contida neles é criptografada ?

- Alguém do grupo de usuários do laboratório leva trabalho para casa ? Caso positivo, alguma informação é passada a um computador pessoal ? Mais alguém tem acesso a estes computadores pessoais ? Existe algum controle de acesso a estas informações de trabalho no computador pessoal ?

1.11. Segurança da rede e comunicações

- Como usuário, você conhece as regras de uso do e-mail de outros funcionários e acesso à Internet por via deste ?

- Você conhece alguém que regularmente viola as restrições de uso do sistema ? Sem nomes, por favor.

- Você já viu pornografia dentro do trabalho ? Pornografia infantil ? Materiais racistas ? Caso positivo, você soube o que fazer ? E o que você fez ?

- Alguém já discutiu as regras de segurança de e-mail com você ? Você sabe como encriptar mensagens importantes ? Você encripta mensagens ?

- Como gerente de rede , você possui diagramas de rede atualizados ? Você pode produzi-lo por demanda ?

- Você sabe quais serviços estão rodando nos seus sistemas conectados à Internet ? Todos eles são necessários ?

- Como você determina quais patches são necessários de se instalar no sistema ? Qual a freqüência de checagem ? Quem é responsável pelo gerenciamento dos patches ? Qual é o intervalo de tempo entre o lançamento de um patch de vulnerabilidade e sua instalação ?

- A sua arquitetura de segurança inclui Firewall ? Caso positivo, o que determina as políticas de segurança instanciadas nas regras de filtragem ?

- Você tem IDS (sistema de detecção de intrusão) ? Quem é o pessoal responsável pela notificação da intrusão ?

- Quais são os procedimentos para resposta a uma intrusão ?

- Se o laboratório usa senhas, como se lida quanto à solicitação de novas senhas ?

- Você tem controle de acesso remoto centralizado ?

- Usuários remotos usam VPNs para acessar, de fora do Firewall, sistemas do laboratório ?

- Os usuários podem usar encriptação para enviar e-mails para a Internet ? Eles usam ? Como você sabe ?

- Os seus usuários aplicam assinatura digital a toda comunicação ?

- Os servidor Web está protegido contra intrusão e vandalismo ?

- A informação sensível encontra-se fora do servidor Web ?

- Você encripta toda informação sensível de dentro do servidor Web ?

- Quanto levaria para você restaurar um servidor Web se este fosse vandalizado ou destruído ?

- Como você sabe que um funcionário foi despedido ou está deixando o emprego ? Quanto leva entre o fim do emprego do funcionário e a sua desativação de acesso a todos os sistemas ?

1.12. Medidas Antivírus

- Você e os outros usuários possuem produtos antivírus em suas estações de trabalho ?

- Qual a freqüência de atualização de antivírus ? Como é feita esta atualização ?

- Quanto tempo leva para que todos os sistemas desatualizados sejam atualizados ?

- Você ou outros usuários abrem anexos de e-mail não solicitados ?

1.13. Backups, arquivos e destruição de dados

- Com qual freqüência é feito o backup das informações ?

- Aonde a mídia de backup é armazenada ? Existem cópias do backup fora do laboratório ? Como você sabe qual mídia utilizar em caso de necessidade de se restaurar um arquivo específico ?

- Por quanto tempo você mantém diferentes tipos de backup ? Por quê ?

- Como você previne acesso não autorizado à mídia de backup ?

- Se você mantém backups por vários anos, como você garante que a mídia antiga será passível de leitura e que os dados desenvolvidos para aplicações antigas serão usados ?

- Como você se desfaz de fitas e discos magnéticos após o ciclo de vida útil destes ter se esgotado ? A mídia descartada é passível de leitura ?

- Você faz cópias de backup de documentos em papel ? Aonde elas são mantidas ? Como você localizaria um determinado documento que necessita ?

- Por quanto tempo você guarda seus papéis ? Por quê ?

- Quando você se desfaz de papéis, o seu conteúdo influencia no modo de destruição deste ? Como você se desfaz de documentos importantes ?

Anexo 2 – Lista de Tabelas

Anexo 3 – Lista de Ilustrações

Referências Bibliográficas

[1] Siyan, K.; Hare, Chris. Internet Firewalls and Network Security. New Riders Publishing. 1995.

[2] RUSecure ISO Information Security Officer´s Manual, versão de avaliação 1.2. Glendale Systems, 2001. Conjunto de programas.

[3] B. Fraser, SITE SECURITY HANDBOOK, RFC 2196, set. 1997. Disponível em: <http://www.ietf.org/rfc/rfc2196.txt?number=2196>. Acesso em: 10 jul. 2002.

[4] D. Henze, IT BASELINE PROTECTION MANUAL, jul. 2001. Disponível em: <http://www.bsi.bund.de/gshb/english/menue.htm>. Acesso em: 10 jul. 2002.

[5] S. Boran, IT SECURITY COOKBOOK, 2001. Disponível em: <http://www.boran.com/security/detail_toc.html>. Acesso em: 20 jul. 2002.

[6] The OpenBSD. Disponível em: <http://www.openbsd.org>. Acesso em: 05 jul. 2002.

[7] B. Caswell e M. Roesch, SNORT – THE OPEN SOURCE NETWORK INTRUSION DETECTION SYSTEM. Disponível em: <http://www.snort.org/>. Acesso em: 05 jul. 2002.

[8] R. Danyliw, ACID – ANALISIS CONSOLE FOR INTRUSION DATABASES: Disponível em: <http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html>. Acesso em: 05 jul. 2002.

[9] S. Garfinkel e G. Spafford, “Practical UNIX and Internet Security”, O’Reilly & Associates, Sebastopol, CA, 1996.

[10] S. Bosworth e M. E. Kabay, “Computer Security Handbook”, 4ª edição, John Wiley and Sons, INC, 2002.

[11] D. B. Chapman e E. D. Zwicky, “Building Internet Firewalls”, 1ª edição, O´Reilly & Associates, Sebastopol, CA, 1995.

[12] Internet Security Systems – ISS. Disponível em: <http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Spoofing/default.htm>. Acesso em: 20 jul. 2002.

[13] C. Hunt, “TCP/IP Network Administration”, 2ª edição, O´Reilly & Associates, Sebastopol, CA, 1997.

[14] G. Fairhurst, ICMP TYPE NUMBERS, 01 out. 2001. Disponível em: <http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/icmp-code.html>. Acesso em: 30 jul. 2002.

[15] M. A. Spohn. Tutorial sobre internet Firewalls, dez. 1996. Disponível em: <http://penta.ufrgs.br/redes296/firewall/packet.html> Acesso em: 05 jul. 2002.

Anexo 4 – Respostas ao Questionário